On finite Dickson near fields

K. Motose

Bull. Fac. Sci. Techn. Hirosaki Univ. 2(2001), 69-78

この論文は H. Zassenhaus による finite Dickson near fields の自己同形決定の証明の簡易化である。

June 2003 本瀬香

Bull. Fac. Sci. Tech. Hirosaki Univ. 2, 69—78 (2001)

On Finite Dickson Near Fields

Kaoru MOTOSE

(Received November 6, 2000)

Finite fields are very useful not only in pure mathematics but also in technology. For example, coding theory, block design, linear modular system, etc. We have a natural question: *Are there algebraic systems like finite fields ?*

Wedderburn proved that there are no finite non-commutative fields, namely, finite division rings are fields. On the other hand, Dickson found some near fields named Dickson near fields, namely, a class of non-commutative fields without one side distributive law.

Finite near fields was classified by H. Zassenhous (see [1] or [2]). In fact, these are Dickson near fields and 7 exceptional near fields.

In this paper, we shall give mainly improvements of his proof to automorphisms of finite Dickson near fields (see [2]).

1. Dickson pairs

The next lemma was found in the text book of elementary number theory.

Lemma 1. *Let $a>1$ be a natural number, let p be a prime and $a\equiv 1 \mod p$.*

(1) *If $p\neq 2$, then $p \parallel \frac{a^p-1}{a-1}$*

(2) *If $p=2$ and $a\equiv 1 \mod 4$ then $2 \parallel \frac{a^p-1}{a-1}$*

(3) *If $p=2$ and $a\equiv 3 \mod 4$ then $4 \mid \frac{a^p-1}{a-1}$*

Proof. We can set $a=pk+1$. In case (1),

$$m=\frac{a^p-1}{a-1}=\sum_{\ell=1}^{p}\binom{p}{\ell}(pk)^{\ell-1}\equiv p\not\equiv 0 \mod p^2 \text{ and } m\equiv 0 \mod p.$$

In case (2), $2 \parallel a+1$. In case (3), $4 \mid a+1$.

A Dickson pair is a foundation of finite Dickson near fields.

Definition. A Dickson pair (D-pair) (q, n) is consist of two natural numbers q and n satisfying the next conditions

(1) $q=p^s$ where p is prime.

(2) every prime factor of n is a divisor of $q-1$.

(3) If $q\equiv 3 \mod 4$ then $n\not\equiv 0 \mod 4$

It is easy to see that if (q, n) is a D-pair and m is a divisor of n, then (q, m) is a D-pair. We

shall denote by $|a|_n$ the order of a mod n

The following theorem is fundamental to construct finite Dickson near fields.

Theorem 1. *Let q be a power of a prime and $n>1$. The following are equivalent.*

(1) *(q, n) is a D-pair*

(2) $\frac{q^n-1}{q-1}\equiv 0 \bmod n$ *and* $\frac{q^k-1}{q-1}\not\equiv 0 \bmod n$ *for* $1\leq k<n$

(3) $n=|q|_{n(q-1)}$

(4) *The next map ν of $\mathbf{Z}/n\mathbf{Z}$ is injective.*

$$\nu : \ell \bmod n \longrightarrow \frac{q^\ell-1}{q-1} \bmod n$$

Proof. (1) $\Rightarrow$ (2): We set $m=s^e\ell$ where s is a prime, $q\equiv 1 \bmod s$ and $(\ell, s)=1$. Then we can see from the next two equations and Lemma 1 that $s^e \| \frac{q^m-1}{q-1}$, in case s is odd or in case $s=2$ and $q\equiv 1 \bmod 4$, and $s^{e+1} \mid \frac{q^m-1}{q-1}$ in case $s=2$ and $q\equiv -1 \bmod 4$.

$$\frac{q^\ell-1}{q-1}=q^{\ell-1}+\cdots+q+1\equiv \ell\not\equiv 0 \bmod s$$

$$\frac{q^m-1}{q-1}=\frac{q^\ell-1}{q-1}\cdot\frac{q^{\ell s}-1}{q^\ell-1}\cdots\frac{q^{\ell s^e}-1}{q^{\ell s^{e-1}}-1}$$

Thus setting $n=m$, we can see $\frac{q^n-1}{q-1}\equiv 0 \bmod n$ by using the only conditions (1) and (2) in the definition of a D-pair.

Assume $\frac{q^m-1}{q-1}\equiv 0 \bmod n$ and $s^f \| n$ with $f\geq 1$. Then $f\leq e$ in case s is odd or in case $s=2$ and $q\equiv 1 \bmod 4$. In case $s=2$ and $q\equiv 3 \bmod 4$, we have $f=1$ by the condition (3) in the definition of a D-pair, and m is even by the next equation.

$$0\equiv\frac{q^m-1}{q-1}=q^{m-1}+\cdots+q+1\equiv m \bmod 2.$$

Thus we obtain n is a divisor of both m and $\frac{q^n-1}{q-1}$.

(2) $\Rightarrow$ (1): We can write $n=n_0n_1$ where every prime divisor of n_1 divides $q-1$ and $(n_0, q-1)=1$. Since (q, n_1) satisfies the conditions (1) and (2) in the definition of a D-pair, using the above, we obtain $q_1=q^{n_1}\equiv 1 \bmod n_1(q-1)$.

Assume $q_1^s\equiv 1 \bmod n_0$. Then $q^{n_1s}\equiv 1 \bmod n_0$ and $q^{n_1s}\equiv 1 \bmod n_1(q-1)$. Thus $q^{n_1s}\equiv 1 \bmod n(q-1)$ by $(n_0, n_1(q-1))=1$. By the assumption, $n_0n_1=n\leq n_1s$ and so $n_0\leq s$. Hence n_0 is the order of q_1 mod n_0 by $q_1^{n_0}=q^n\equiv 1 \bmod n_0$. Thus n_0 is a divisor of $\varphi(n_0)$ by the Euler's theorem. This means $n_0=1$ and every prime divisor of $n=n_1$ divides $q-1$.

Assume that $q\equiv 3 \bmod 4$ and $n=2^e\ell$ where $e\geq 2$ and ℓ is odd. Since (q, ℓ) is a D-pair, we have $\frac{q^\ell-1}{q-1}\equiv 0 \bmod \ell$. Thus

$$\frac{q^{n/2}-1}{q-1}=\frac{q^{n/2}-1}{q^\ell-1}\cdot\frac{q^\ell-1}{q-1}\equiv 0 \bmod \ell.$$

On the other hand, we have $\frac{q^{n/2}-1}{q-1}\equiv 0 \bmod 2^e$ from the equations

$$\frac{q^{n/2}-1}{q-1}=\frac{q^\ell-1}{q-1}\cdot\frac{q^{2\ell}-1}{q^\ell-1}\cdots\frac{q^{2^{e-1}\ell}-1}{q^{2^{e-2}\ell}-1} \text{ and } \frac{q^{2\ell}-1}{q^\ell-1}\equiv 0 \bmod 4.$$

Thus we obtain the next contradiction and so $e \leq 1$.

$$\frac{q^{n/2}-1}{q-1} \equiv 0 \bmod n$$

(2) $\Leftrightarrow$ (3) and (2) $\Leftrightarrow$ (4) are easy to prove.

The next needs later for automorphisms of finite Dickson near fields.

Proposition 1. *Let* (q, n) *be a D-pair. We set* $m=\frac{q^n-1}{n}$ *and* $t=\frac{m}{q-1}$. *Then*

1. $(n, t)=\begin{cases} 2 & \text{in case } q \equiv -1 \bmod 4 \text{ and } n=2n_0 \text{ where } n_0 \text{ is odd} \\ 1 & \text{in another case} \end{cases}$

2. $n=|q|_t$ *if* $(q, n) \neq (3, 2)$

Proof. We may assume $q \geq 3$ since (q, n) is a D-pair. We set $n=r^e n_0$ where r is prime, $(n_0, r)=1$ and $e \geq 1$.

Proof of 1: Assume r is odd. Then we have

$$r^e \parallel \frac{q^n-1}{q-1}$$

Thus t is not divided by r.

Assume $r=2$.

In case $q \equiv 1 \bmod 4$,

$$2^e \parallel \frac{q^n-1}{q-1}$$

Thus t is odd.

In case $q \equiv -1 \bmod 4$ and $n=2n_0$, where n_0 is odd, we have $q^{n_0} \equiv -1 \bmod 4$ and so

$$4 \mid (q^{n_0}+1) \cdot \frac{q^{n_0}-1}{q-1} = \frac{q^n-1}{q-1}$$

This means t is even.

Proof of 2: Next we shall prove $n=|q|_t$ if $(q, n) \neq (3, 2)$. Noting that $q^n \equiv 1 \bmod t$, we can set $n=sk$, $k \geq 2$ for $s=|q|_t$. Since $q^s \equiv 1 \bmod t$, we have

$$n(q^s-1) = \ell \cdot \frac{q^n-1}{q-1}$$

for some ℓ. Assume $\ell \geq 2$. Then we have a contradiction $s > 3^{s-1}$ from the next.

$$s \geq \frac{2}{k(q-1)} \cdot \frac{(q^s)^k-1}{q^s-1} > \frac{2}{kq}\left((q^s)^{k-1}+\cdots+q^s+1\right) > \frac{2(k-1)}{k} q^{s-1} \geq 3^{s-1}$$

Hence $\ell=1$ and

$$n = \frac{q^n-1}{(q^s-1)(q-1)}$$

We set $r^e \parallel n$. In case r is odd or in case $r=2$ and $q \equiv 1 \bmod 4$, we have $r^e \parallel \frac{q^n-1}{q-1}$ contrary to $r^{e+1} \mid n(q^s-1)=\frac{q^n-1}{q-1}$. Thus $q \equiv 3 \bmod 4$ and so $n=2$ since (q, n) is a D-pair. Therefore $2(q-1)=\frac{q^2-1}{q-1}$ and so $q=3$.

2. Dickson near fields

We shall give the definition of finite Dickson near fields in the next theorem.

Theorem 2. *Let (q, n) be a D-pair, let F_{q^n} be a finite field of order q^n, let $\rho : x \to x^q$ be an automorphism of F_{q^n} and let ω be a generator of the multiplicative group $F_{q^n}^*$. We define $\rho_a = \rho^{s'}$ for $a \in F_{q^n}^*$, where $\frac{q^{s'}-1}{q-1} \equiv s \bmod n$ for $a = \omega^s$. Then we can construct a Dickson near field D_{q^n} by the sum and the next new product $\circ$ in F_{q^n}. For $a, b \in F_{q^n}$,*

$$a \circ b = \begin{cases} a\rho_a(b) & \text{for } a \neq 0 \\ 0 & \text{for } a = 0 \end{cases}$$

Proof. First, we shall prove

$$\rho_{a \circ b} = \rho_a \rho_b \text{ for } a, b \in F_{q^n}^*.$$

We set $a = \omega^s$, $b = \omega^t$ and $\frac{q^{s'}-1}{q-1} \equiv s$, $\frac{q^{t'}-1}{q-1} \equiv t \bmod n$. Then we have

$$s + tq^{s'} \equiv \frac{q^{s'}-1}{q-1} + \frac{q^{t'}-1}{q-1} q^{s'} = \frac{q^{s'+t'}-1}{q-1} \bmod n$$

Thus we obtain $\rho_{a \circ b} = \rho_a \rho_b$ from the next equation.

$$\rho_{a \circ b} = \rho_{a\rho_a(b)} = \rho_{ab^{q^{s'}}} = \rho_{\omega^{s+tq^{s'}}} = \rho^{s'+t'} = \rho_a \rho_b$$

For $a, b \in D_{q^n}^*$, we can see

$$(a \circ b) \circ c = (a \circ b)\, \rho_{a \circ b}(c) = (a\rho_a(b))\, \rho_a(\rho_b(c)) = a\rho_a(b\rho_b(c)) = a \circ (b \circ c)$$

It is easy to prove the associative law for $a = 0$ or $b = 0$.
For $a \in D_{q^n}^*$, we can see

$$a \circ (b+c) = a\rho_a(b+c) = a(\rho_a(b) + \rho_a(c)) = a\rho_a(b) + a\rho_a(c) = a \circ b + a \circ c$$

It is easy to prove the left distributive law for $a = 0$. We can see also

$$1 \circ a = a \circ 1 = a \text{ for } a \in D_{q^n}.$$

Thus D_{q^n} is a finite near ring with the identity 1.
On the other hand $a \circ b = a\rho_a(b) \neq 0$ for $a \neq 0$ and $b \neq 0$.
It is easy to prove $D_{q^n}^*$ is a group and D_{q^n} is a near field.

The next lemma is very useful.

Lemma 2. *Let p be prime, let $q = p^\ell$ and let ω be a generator of the multiplicative group $F_{q^n}^*$. Then $F_{q^n} = F_p(\omega^n)$.*

Proof. Let p^f be the order of $F_p(\omega^n)$. Then f is a divisor of ℓn. Since $F_p(\omega^n)$ contains ω^n, $\omega^{n(p^f-1)} = 1$. Hence $p^{\ell n} - 1$ is a divisor of $n(p^f-1)$ and so

$$n(p^f-1) \geq p^{\ell n}-1=(p^{(\ell n)/2}+1)(p^{(\ell n)/2}-1) > n(p^{(\ell n)/2}-1)$$

Thus $p^f > p^{(\ell n)/2}$ and $2 > \frac{\ell n}{f}$. Hence $f = \ell n$.

The center of D_{q^n} is determined by the above lemma.

Proposition 2. *F_q is the center of D_{q^n}.*

Proof. Let ζ be an element in the center of D_{q^n}. Then

$$\zeta \rho_\zeta(\omega^n)=\zeta \circ \omega^n=\omega^n \circ \zeta=\omega^n \rho_{\omega^n}(\zeta)=\omega^n \zeta.$$

Thus $\rho_\zeta(\omega^n)=\omega^n$. By Lemma 2, $D_{q^n}=F_p(\omega^n)$ and $\rho_\zeta=1$. Hence we obtain

$$\zeta_\omega=\zeta \rho_\zeta(\omega)=\zeta \circ \omega=\omega \circ \zeta=\omega \rho_\omega(\zeta)=\omega \rho(\zeta)=\omega \zeta^q$$

Hence $\zeta \in F_q$. On the other hand let $\alpha \in F_q^*=<\omega^{\frac{q^n-1}{q-1}}>$. Then $\alpha=\omega^{\frac{q^n-1}{q-1}k}$ and so $\rho_\alpha=1$. Thus we obtain for $b=\omega^r$,

$$b \circ \alpha=b\rho_b(\alpha)=b\rho^r(\alpha)=b\alpha^{q^r}=\alpha b=\alpha \rho_\alpha(b)=\alpha \circ b.$$

It is easy to see $\alpha \circ 0=0=0 \circ \alpha$. Therefore we have the conclusion.

3. Near fields and Sharply 2-transitive groups

In this section, finite near fields are nothing but sharply 2-transitive groups on a finite sets.

Let K be a near field, and let $G=\{x \to ax+b \mid a \in K^*, b \in K\}$. Then G is a permutation group on K. Let u_a, v_a be elements in G such that

$$u_a : x \longrightarrow x+a, \quad v_a : x \longrightarrow ax$$

Then $\varepsilon=u_0=v_1 : x \to x$ is the identity map. We set the subgroups

$$U=\{u_a \mid a \in K\}, \quad V=\{v_a \mid a \in K^*\}$$

Then $G=UV$, $G \triangleright U$, $U \cap V=\{\varepsilon\}$. It is easy to see that U consist of u_0 and fixed point-free permutations and $V=G_0 \neq \{\varepsilon\}$. Since G is transitive on K and G_0 is transitive on K^*, we can see G is 2-transitive on K. $G_0 \neq \{\varepsilon\}$ and $G_{a,b}=\{\varepsilon\}$ for $a \neq b$.

Conversely, we assume that G is 2-transitive on a finite set $K=\{0, 1, \ldots, n-1\}$, $G_0 \neq \{\varepsilon\}$ and $G_{a,b}=\{\varepsilon\}$ for $a \neq b \in K$. Then we can set a structure of a near field in a set K by the following method.

It is easy to see that for $a \in K^*=K \setminus \{0\}$, there exists only one $v_a \in V=G_0$ with $v_a(1)=a$. We define sum and product of elements a, b in K by the above v_a and the next u_a defined in Lemma 3.

$$a+b := u_b(a), \quad ab := v_a(b) \text{ for } a \neq 0 \text{ and } 0b := 0$$

The following lemma shows some properties of the above group G.

Lemma 3. *Let G be a sharply 2-transitive group on $K=\{0, 1, \ldots, n-1\}$ and let U be the set consisting of the identity and fixed point-free permutations. Then*

(1) *U is a normal subgroup of G.*

(2) *U is elementary abelian.*

Proof. (1) It is easy to see $\rho U\rho^{-1}=U$ for all $\rho\in G$. First we shall prove, for $k\in K^*$, there exists only one $u_k\in U$ with $u_k(0)=k$, equivalently, the next map ν from U to K is bijective.

$$\nu : u \longrightarrow u(0)$$

For $\tau\in U-\{1\}$, there exists $\rho\in G_0$ with $\rho(\tau(0))=k$ since $\tau(0)\neq 0$ and G_0 is transitive on K^*. We set $u_k=\rho\tau\rho^{-1}$. Then $u_k\in U$ and $u_k(0)=k$. Thus ν is surjective. It follows from definition of G and U that

$$U=G-\bigcup_{a\in K}(G_a-1), \qquad (G_a-1)\cap(G_b-1)=\emptyset \text{ for } a\neq b$$

Using $|G| = |G_a||a^G| = |G_a||K|$, we can see $|U|=|K|$. Hence ν is injective.

Assume $\sigma\tau$ has a fixed point ℓ for σ, $\tau\in U$. Then we may assume $\ell=0$ since G is transitive on K. Thus $\tau=\sigma^{-1}$ follows from $\sigma^{-1}\in U$, $\tau(0)=\sigma^{-1}(0)$ and the above observation. This means $\sigma\tau\in U$. Hence U is a normal subgroup of G.

(2) Let p be a prime factor of $|U|$ and let τ be an element of order p in the center of p-Sylow subgroup of U. We set $\sigma\in U-\{1\}$. Then there exists $\rho\in G_0$ with $\rho(\tau(0))=\sigma(0)$. Thus $\rho\tau\rho^{-1}=\sigma$ follows from $\rho\tau\rho^{-1}\in U$ and $\rho\tau\rho^{-1}(0)=\sigma(0)$. Thus the order of every element in U is p or 1 and so σ is in the center of a p-group U. Thus U is elementary abelian.

The next shows K is a near field.

Theorem 3. *K is a near field by the above definition of sum and product.*

Proof. First we shall prove the next equations:

$$u_au_b=u_{b+a}, \qquad v_av_b=v_{ab} \qquad v_au_bv_a^{-1}=u_{ab}$$

These follow from

$$u_au_b(0)=u_a(b)=b+a=u_{b+a}(0),\ v_av_b(1)=v_a(b)=ab=v_{ab}(1), \text{ and}$$
$$v_au_bv_a^{-1}(0)=v_au_b(0)=v_a(b)=ab=u_{ab}(0)$$

Next we shall prove the next from the first equation and U is commutative.

$$a+(b+c)=u_{b+c}(a)=u_cu_b(a)=u_c(a+b)=(a+b)+c$$
$$a+b=u_{a+b}(0)=u_bu_a(0)=u_au_b(0)=u_a(b)=b+a$$
$$a+0=0+a=u_a(0)=a$$
$$a+u_a^{-1}(0)=u_a^{-1}(0)+a=u_a(u_a^{-1}(0))=\varepsilon(0)=0$$

We shall prove the next from the second equation for $a, b \in K^*$. For $a=0$ or $b=0$, it is easy to prove our equations.

$$a(bc)=v_a(bc)=v_a(v_b(c))=v_av_b(c)=v_{ab}(c)=(ab)c$$
$$a1=v_a(1)=a=\varepsilon(a)=v_1(a)=1a$$
$$av_a^{-1}(1)=v_a(v_a^{-1}(1))=\varepsilon(1)=1$$

For $a\in K^*$, $v_a^{-1}(1)\neq 0$ follows from $v_a(0)=0\neq 1$ and we can see $v_{v_a^{-1}(1)}=v_a^{-1}$ by $v_{v_a^{-1}(1)}(1)=v_a^{-1}(1)$. Thus we have

$$v_a^{-1}(1)a=v_{v_a^{-1}(1)}(a)=v_a^{-1}(a)=v_a^{-1}(v_a(1))=1$$

The next follows from the third equation

$$a(b+c)=v_a(b+c)=v_a(u_c(b))=v_au_cv_a^{-1}(v_a(b))=u_{ac}(ab)=ab+ac$$

Thus K is a near field by our definition of sum and product.

4. Structure of the multiplicative group of a Dickson near field

The next gives the structure of the multiplicative group of a Dickson near field.

Theorem 4. *Let D_{q^n} be a Dickson near field. Then $D_{q^n}^*$ is meta-cyclic with generators $b=\omega$, $a=\omega^n$ satisfying the next relations in $D_{q^n}^*$.*

$$a^m=1,\ b^n=a^t,\ bab^{-1}=a^q,\ \text{where } m=\frac{q^n-1}{n},\ t=\frac{m}{q-1}$$

Proof. It follows from $\rho_{x\circ y}=\rho_x\rho_y$ that $\nu: x\to\rho_x$ is a homomorphism from $D_{q^n}^*$ to the automorphism group of F_{q^n} over F_q. It is easy to see Ker $\nu=<a>$ and the factor group $D_{q^n}^*/\text{Ker }\nu$ is generated by the class of ω.

It is easy to see from $a\circ x=ax$ for $x\in D_{q^n}$ that m is the order of a. The second equation $b^n=a^{\frac{m}{q-1}}$ follows from the next

$$b^n=\overbrace{\omega\circ\omega\circ\cdots\circ\omega}^{n\text{ times}}=a^{\frac{m}{q-1}}\in<a>\ \text{and so}\ b^n\circ x=b^nx\ \text{for}\ x\in D_{q^n}.$$
$$ba=\omega\circ\omega^n=\omega\rho_\omega(\omega^n)=\omega\rho(\omega^n)=\omega^{q^n+1}=a^qb$$

We set $G=D_{q^n}^*=<a, b\mid a^m=1, b^n=a^t, bab^{-1}=a^q>$, where (q, n) is a D-pair, $m=\frac{q^n-1}{n}$ and $t=\frac{m}{q-1}$.

The next proposition is important in Proposition 4.

Proposition 3. *The subgroup $<a^t>$ is the center of G.*

Proof. It follows from Proposition 2 that F_q^* is the center of G. Since the order of a^t is $q-1$, we have $<a^t>=F_q^*$.

Let $\bar{G}=G/<a^t>$ and let σ be an automorphism of G. Then

$$\bar{G}=<\bar{a}, \bar{b}\mid \bar{a}^t=1,\ \bar{b}^n=1,\ \bar{b}\,\bar{a}\,\bar{b}^{-1}=\bar{a}^q>$$

and $\bar{\sigma}$ is an automorphism of $\bar{G}$ defined by $\bar{\sigma}(\bar{x}) = \overline{\sigma(x)}$ for $x \in G$.

The next needs for automorphisms of finite Dickson near fields

Proposition 4. *We set*

$$a_1 = \begin{cases} a^2 & \text{in case } q \equiv -1 \bmod 4 \text{ and } n = 2n_0 \text{ where } n_0 \text{ is odd} \\ a & \text{in another case} \end{cases}$$

Then the subgroup $\langle a_1 \rangle$ *is characteristic in* G.

Proof. If $(q, n) = (3, 2)$, then $t = 2$ and $\langle a^2 \rangle$ is the center of G. So we may assume $(q, n) \neq (3, 2)$. Let σ be an automorphism of G and let $\bar{\sigma}(\bar{a}) = \bar{a}^k \bar{b}^\ell$. Then it follows from the next that $\bar{b}^{t\ell} \in \langle \bar{a} \rangle$.

$$1 = (\bar{a}^k \bar{b}^\ell)^t = \bar{a}^{k\frac{q^{\ell t}-1}{q^\ell - 1}} \bar{b}^{t\ell}$$

Hence $\bar{a} = \bar{b}^{t\ell} \bar{a} \bar{b}^{-t\ell} = \bar{a}^{q^{t\ell}}$. Thus $q^{t\ell} \equiv 1 \bmod t$ and hence by Proposition 1, $t\ell \equiv 0 \bmod n$.

In case $(n, t) = 1$, we have $\ell = n\ell_0$. Thus

$$\overline{\sigma(a)} = \bar{\sigma}(\bar{a}) = \bar{a}^k \bar{b}^\ell = \bar{a}^k (\bar{b}^n)^{\ell_0} = \bar{a}^k$$

Hence we have $\sigma(a) \in \langle a \rangle$.

In case $(n, t) = 2$, we have $t_0 \ell \equiv 0 \bmod n_0$ and $\ell = n_0 \ell_0$, where $t = 2t_0$ and $n = 2n_0$. Thus

$$\overline{\sigma(a^2)} = \bar{\sigma}(\bar{a}^2) = (\bar{a}^k \bar{b}^\ell)^2 = \bar{a}^{k(1+q^\ell)} \bar{b}^{2\ell} = \bar{a}^{k(1+q^\ell)} (\bar{b}^n)^{\ell_0} = \bar{a}^{k(1+q^\ell)}$$

Hence we have $\sigma(a^2) \in \langle a^2 \rangle$ since $1 + q^\ell$ and t are even.

5. Automorphisms of Dickson near fields

The next lemma needs later.

Lemma 4. *If* $F_{q^*} \neq F_q(a_1)$, *then* $(q, n) = (3, 2)$.

Proof. It follows from Lemma 2 and setting of a_1 (see Proposition 4) that $a_1 = a^2$, $n = 2n_0$, $[F_q(a_1) : F_q] = n_0$ and $m = t(q-1)$ is even. Since $a_1 \in F_q(a_1)$ and the order of a_1 is $m_0 = \frac{m}{2}$, we have m_0 is a divisor of $q^{n_0} - 1$.

$$4n_0 = 2n = (q^{n_0} + 1)\frac{q^{n_0} - 1}{m_0} \geq q^{n_0} + 1 \geq 3^{n_0} + 1$$

It follows from these inequalities that $n_0 = 1$ and $q = 3$, namely, $(q, n) = (3, 2)$.

The following theorem characterizes automorphisms of finite Dickson near fields.

Theorem 5. *Assume* $(q, n) \neq (3, 2)$. *We set* $q = p^e$ *where* p *is a prime and* $h = |p|_n$. *Let* D_{q^*} *be a Dickson near field and let* $\nu : x \to x^p$ *be an automorphism of* F_{q^*}. *Then* σ *is an automorphism of* D_{q^*} *if and only if* $\sigma = \nu^s$ *for some* $s \equiv 0 \bmod h$.

Proof. Let σ be an automorphism of D_{q^*}. We saw in Lemma 4 that $F_{q^*} = F_p(a_1)$ where ω

is a generator of F_q^*, $a=\omega^n$ and a_1 was defined in Proposition 4. If $f(x)$ is the minimum polynomial of a_1 over F_p, then $f(x)$ is also the minimum polynomial of $\sigma(a_1)$ over F_p because $a_1, \sigma(a_1) \in <\omega^n>$ by Proposition 4 and so $a_1 \circ y = a_1 y$, $\sigma(a_1) \circ z = \sigma(a_1) z$. Hence σ is an automorphism of F_q. and $\sigma = \nu^s$ for some s.

On the other hand, there exists d with $\sigma(d)=c$ for an arbitrary $c \in F_q$.

$$\begin{aligned}\sigma(\omega)\rho_\omega(c) &= \sigma(\omega)\rho_\omega(\sigma(d)) = \sigma(\omega)\sigma\rho_\omega(d) = \sigma(\omega\rho_\omega(d)) \\ &= \sigma(\omega \circ d) = \sigma(\omega) \circ \sigma(d) = \sigma(\omega)\rho_{\sigma(\omega)}(\sigma(d)) \\ &= \sigma(\omega)\rho_{\sigma(\omega)}(c)\end{aligned}$$

Therefore

$$\rho_\omega = \rho_{\sigma(\omega)}$$

We set

$$\frac{q^{(p^s)'}-1}{q-1} \equiv p^s \bmod n$$

$\rho^{(p^s)'} = \rho_{\sigma(\omega)} = \rho_\omega = \rho$. Thus $(p^s)' \equiv 1' \bmod n$. By Theorem 1, we have $p^s \equiv 1 \bmod n$. Thus $s \equiv 0 \bmod h$.

Conversely, we assume that $\sigma = \nu^s$ for some $s \equiv 0 \bmod h$. We set $c=\omega^k$ where ω is a generator of F_q^*. Then $\sigma(c) = \omega^{kp^s}$ and by the condition, we have $p^s k \equiv k \bmod n$ since $p^s \equiv 1 \bmod n$. Thus

$$\frac{q^{(p^s k)'}-1}{q-1} \equiv p^s k \equiv k \equiv \frac{q^{k'}-1}{q-1} \bmod n$$

Thus $(p^s k)' \equiv k' \bmod n$ by Theorem 1 and so $\rho_{\sigma(c)} = \rho^{(p^s k)'} = \rho^{k'} = \rho_c$ for all $c \in F_q^*$. Hence we have for $c \in F_q^*$

$$\begin{aligned}\sigma(c \circ d) &= \sigma(c\rho_c(d)) = \sigma(c)\sigma(\rho_c(d)) = \sigma(c)\sigma\rho_c(d) \\ &= \sigma(c)\rho_c\sigma(d) = \sigma(c)\rho_{\sigma(c)}\sigma(d) \\ &= \sigma(c) \circ \sigma(d)\end{aligned}$$

It is easy to see the equation $\sigma(0 \circ d) = \sigma(0) \circ \sigma(d)$.

The next proposition provides the automorphism group of D_{3^2}

Proposition 5. *The automorphism group* $\mathrm{Aut}(D_{3^2})$ *of* D_{3^2} *is isomorphic to the symmetric group* S_3 *of degree* 3.

Proof. We set $F_{3^2} = F_3[x]/(x^2+1)$ and $i = \bar{x}$ is the class of x. Let τ, σ be automorphisms of the additive group of D_{3^2} defined by

$$\tau(\alpha+\beta i) := \alpha - \beta i, \quad \sigma(\alpha+\beta i) := \alpha+\beta+\beta i \text{ for } \alpha+\beta i \in D_{3^2}$$

where $\alpha, \beta \in F_3$ and $i^2=-1$. Then it is easy see

$$<\sigma, \tau \mid \sigma^3=1, \tau^2=1, \tau\sigma\tau^{-1}=\sigma^2> \cong S_3$$

We set $\omega := 1-i$, $b := \omega$, $a := \omega^2 = i$. Then ω is a generator of $F_{3^2}^*$ and we can see from the definition of D_{3^2},

$$\omega^k \circ x = \begin{cases} \omega^k x & \text{if } k \text{ is even} \\ \omega^k x^3 & \text{if } k \text{ is odd} \end{cases}$$

It follows from Theorem 4 and $a^2 = -1$ that

$$D_{3^2}^* = \langle a, b \mid b^2 = a^2 = -1, bab = a \rangle$$

If ν is an automorphism of D_{3^2}, then ν fixes all elements of F_3 and so ν is determined by $\nu(i) = \lambda + \eta i$, where λ, $\eta \in F_3$. It is easy to see $\eta \neq 0$. Thus $|\mathrm{Aut}(D_{3^2})| \leq 6$. If τ, σ are automorphisms of D_{3^2}, then we have the conclusion

$$\mathrm{Aut}(D_{3^2}) \cong S_3$$

First we shall prove that τ is an automorphism of D_{3^2}.

$$\tau(a) = \tau(i) = -i = -a, \quad \tau(b) = \tau(1-i) = 1+i = ab$$

Noting $a^2 = (ab)^2 = b^2 = -1$, we have

$$\tau(a)^2 = \tau(b)^2 = -1, \quad \tau(b)\tau(a)\tau(b) = ab(-a)ab = -a = \tau(a)$$

Next we shall prove that σ is an automorphism of D_{3^2}.

$$\sigma(a) = \sigma(i) = 1+i = \omega^2 \circ \omega = ab, \quad \sigma(b) = \sigma(1-i) = -i = -a$$

Noting $(ab)^2 = a^2 = -1$ and $-ba = ab$, we have

$$\sigma(a)^2 = \sigma(b)^2 = -1, \quad \sigma(b)\sigma(a)\sigma(b) = (-a)ab(-a) = ab = \sigma(a)$$

References

[1] G. Pilz, Near rings, Mathematics Studies 23, North-Holland, 1977

[2] H. Zassenhaus, Über endliche Fastkörper, Abh. Math. Sem. Univ. Hamburg 11 (1935/36), 187–220.

Department of Mathematical System Science,
Faculty of Science and Technology,
Hirosaki University,
Hirosaki 036-8561, Japan
E-mail address skm@cc.hirosaki-u.ac.jp