On finite Dickson near-fields

SUSAN DANCS

A near-field $K(+, \circ)$ is called a *Dickson near-field* if a third binary operation $\cdot$ can be defined on K, such that $K(+, \cdot)$ is a skew field and, for each $a \in K^*$, $\varphi_a : x \to a^{-1} \cdot (a \circ x)$ is an automorphism of $K(+, \cdot)$, where a^{-1} denotes the inverse of a in the skew field $K(+, \cdot)$. (See H. KARZEL [3].)

Such near-fields were first constructed by L. E. DICKSON [1]. H. ZASSENHAUS [4] showed that, with seven exceptions, Dickson's method yields all finite near-fields. The results of E. ELLERS and H. KARZEL [2] show that these correspond precisely to the finite Dickson near-fields.

A finite Dickson near-field has order q^n and centre of order q. It is completely specified, up to isomorphism, by the positive integer invariants q, n. Furthermore, q and n satisfy the following relations:

(1) $q = p^l$ *for some prime* p;

(2) *each prime divisor of* n *divides* $q - 1$;

(3) *if* $q \equiv 3 \bmod 4$, *then* $n \not\equiv 0 \bmod 4$.

Such a pair of integers $\{q, n\}$ is called a Dickson number pair and, for each Dickson number pair, there exists a Dickson near-field with invariants q, n.

The following results will be proved here.

Theorem. *Let* K *be a finite Dickson near-field with invariants* p^l, n. *For each* λ *dividing* ln, K *has a sub-near-field* N *of order* p^λ, *isomorphic to the Dickson near-field with invariants* $p^{l'}, \lambda/l'$, *where* $l' = (lI, \lambda)$ *and* I *is the solution of* $I \equiv (p^{ln} - 1)/(p^\lambda - 1) \bmod n$ *such that* $0 < I \leq n$.

Those sub-near-fields of K which contain the centre are of particular interest. For these, the invariants are easier to describe.

Corollary. *If* $\lambda = lt$, *for some integer* t, *then* N *contains the centre of* K *and* $l' = l(n/t, t)$.

It should be noted that K contains no sub-near-fields other than those described in the theorem (see Bull. Austral. Math. Soc. 5 (1971), 275—280).

§ 1. The Dickson-Zassenhaus Construction

A brief outline of the Dickson-Zassenhaus construction is needed. For a detailed description see p. 190 of ZASSENHAUS [4].

Let $\{q, n\}$ be a Dickson number pair. Then

(4) $$\frac{q^{\beta}-1}{q-1} \not\equiv 0 \bmod n \quad \text{for} \quad 0 < \beta < n, \quad \frac{q^{n}-1}{q-1} \equiv 0 \bmod n.$$

Hence, the congruence equation

(5) $$q^{\alpha} \equiv 1 + \mu(q-1) \bmod (q-1)n$$

has a unique solution for all μ, such that $0 < \alpha \leq n$.

Let $K(+, \cdot)$ be the finite field with q^n elements, ω a generator of its multiplicative group $K^*(\cdot)$ and let ϱ be the automorphism of $K(+, \cdot)$ defined by $\varrho : x \to x^q$. A mapping $\varphi : x \to \varphi_x$, from K^* into the automorphism group of $K(+, \cdot)$, is defined by $\varphi_x = \varrho^{\alpha}$ for $x = \omega^{\mu}$, where α is the solution of (5). Define a multiplication $\circ$ by

(6) *for* $a, b \in K$, $a \circ b = a \cdot \varphi_a(b)$, *for* $a \neq 0$, *and* $a \circ b = 0$, *for* $a = 0$.

$K(+, \circ)$ is a near-field with q^n elements and centre isomorphic to the finite field of order q. Furthermore, $K(+, \circ)$ is clearly a Dickson near-field. Moreover, for a given Dickson number pair $\{q, n\}$, $K(+, \circ)$ is unique up to isomorphism. The image, $\Gamma = \varphi(K^*)$, of K^* under φ is the cyclic group of order n generated by ϱ and is called the *D-group* of $K(+, \circ)$.

§ 2. Number theoretic lemmas

Lemma 2.1. *Let* $\{q, n\}$ *be a Dickson number pair. If* k *divides* n, *then* $\{q^k, k\}$ *is a Dickson number pair.*

This results is an immediate consequence of the observation that (3) is equivalent to the following condition:

(3′) *if* 4 *divides* n, *then* 4 *divides* $q - 1$.

Lemma 2.2. *Let* $\{q, n\}$ *be a Dickson number pair. If* $q^{\alpha} \equiv 1 + \mu(q-1) \bmod (q-1)n$, *then* $(\mu, n) = (\alpha, n)$.

Proof. Let $(\mu, n) = \xi$ and $(\alpha, n) = \eta$. By Lemma 2.1, $\{q, \xi\}$ and $\{q, \eta\}$ are Dickson number pairs. Since $(q^{\alpha}-1)/(q-1) \equiv \mu \bmod n$, $(q^{\alpha}-1)/(q-1) \equiv 0 \bmod \xi$. Hence, by (4), $\xi \mid \alpha$. But $\xi \mid n$ and hence $\xi \mid \eta$.

Again, by (4), since $\eta \mid \alpha$, $(q^{\alpha}-1)/(q-1) \equiv 0 \bmod \eta$. Thus $\mu \equiv \varkappa\eta$ mod n, for some integer $\varkappa$. Hence $\eta \mid \mu$. But $\eta \mid n$, so $\eta \mid \xi$, Thus $\xi = \eta$.

Lemma 2.3. *If $\{q, n\}$ is a Dickson number pair and t divides n, then* $(q^n - 1)/(q^t - 1) \equiv n/t \bmod n$.

Proof. Let $n/t = s = s_1 s_2 \ldots s_r$, where s_i is prime for $i = 1, 2, \ldots, r$. The proof is obtained by induction on r.

Let $r = 1$. Then $n/t = s$, where s is prime. By Lemma 2.1, $\{q, t\}$ is a Dickson number pair. Hence $q^t \equiv 1 \bmod (q-1)t$. But s is prime and $s \mid n$, thus, by (2), $s \mid q - 1$. Hence $q^t \equiv 1 \bmod n$, since $n = st$. But

$$(q^n - 1)/(q^t - 1) = (q^{st} - 1)/(q^t - 1) = q^{t(s-1)} + q^{t(s-2)} + \cdots + q^t + 1.$$

Thus $(q^n - 1)/(q^t - 1) \equiv s \bmod n$, as required.

Let $r > 1$. Then $n = st = s_1 s' t$, where s_1 is prime. By above, $(q^{s_1 s' t} - 1)/(q^{s' t} - 1) \equiv s_1 \bmod n$. Further, since $\{q, s' t\}$ is a Dickson number pair, $(q^{s' t} - 1)/(q^t - 1) \equiv s' \bmod s' t$, by the inductive hypothesis. The result follows.

The proofs of the following two lemmas require only routine calculations and are omitted.

Lemma 2.4. *If $(b, c) = (d, c)$, then $(ab, c) = (ad, c)$.*

Lemma 2.5. *If $a \neq 0$ and $(b, ca) = (d, ca)$, then $(b, c) = (d, c)$.*

§ 3. Proof of the theorem

Lemma 3.1. *Let K be a finite Dickson near-field with invariants p^l, n. Then K contains a Dickson near-field of order p^λ, for each λ dividing ln.*

Proof. Let $N(+, \cdot)$ be the (unique) sub-field of $K(+, \cdot)$ of order p^λ, where $\lambda \mid ln$. Let $a, b \in N^*$. Then $a \circ b = a \cdot \varphi_a(b) = a \cdot b^{q^\alpha}$, for some α, so $a \circ b \in N^*$. Thus, since K^* is finite, $N^*(\circ)$ is a subgroup of $K^*(\circ)$ and $N(+, \circ)$ is a sub-near-field of $K(+, \circ)$. Since N admits φ_a, the restriction, $\varphi_a|_N$, of φ_a to N is an automorphism of $N(+, \cdot)$. Hence $N(+, \circ)$ is a Dickson near-field.

Lemma 3.2. *If $\bar\omega$ is a generator of $K^*(\cdot)$, then $\varphi_{\bar\omega}$ is a generator of Γ, the D-group of $K(+, \circ)$.*

Proof. Since $\bar\omega$ generates $K^*(\cdot)$, $\bar\omega = \omega^{\bar\mu}$ where $(\bar\mu, q^n - 1) = 1$. By (4), $n \mid q^n - 1$. Thus $(\bar\mu, n) = 1$. Hence, by Lemma 2.2, $(\bar\alpha, n) = 1$, where $\varrho^{\bar\alpha} = \varphi_{\bar\omega}$, and $\varphi_{\bar\omega}$ generates Γ.

Let N be the sub-near field of K of order p^λ given by Lemma 3.1 and let its invariants be $p^{l'}, n'$, where $n' = \lambda/l'$. To prove the theorem, it ... that l' has the required properties.

Since $N^*(\cdot)$ is a cyclic subgroup of $K^*(\cdot)$ of order $p^\lambda - 1$, if ω generates $K^*(\cdot)$, then $\bar{\omega} = \omega^i$ generates $N^*(\cdot)$, where $i = (p^{ln} - 1)/(p^\lambda - 1)$. Let I be the solution of the congruence equation $I \equiv i \bmod n$, such that $0 < I \leq n$.

Also, since N is a Dickson near-field, there exists a mapping ψ from N^* into the automorphism group of $N(+,\cdot)$ and a generator $\bar{\omega}^\sigma$ of $N^*(\cdot)$, such that $\bar{\varrho} = \psi_{\bar{\omega}^\sigma} : x \to x^{p^{l'}}$. Then the D-group, $\Pi = \psi(N^*)$, of $N(+,\circ)$ is generated by $\bar{\varrho}$ and has order n'. Furthermore, for all $a \in N$, $\bar{\omega} \circ a = \bar{\omega} \cdot \psi_{\bar{\omega}}(a)$. But $\bar{\omega} \circ a = \bar{\omega} \cdot \varphi_{\bar{\omega}}(a)$ and hence $\psi_{\bar{\omega}} = \varphi_{\bar{\omega}}|_N$. By (5), $\varphi_{\bar{\omega}} = \varrho^\alpha$, where $\varrho : x \to x^{p^l}$ and α satisfies $q^\alpha \equiv 1 + i(q - 1) \bmod (q - 1)n$. Hence $\psi_{\bar{\omega}} : x \to x^{p^{l\alpha}}$ for all $x \in N$. By Lemma 3.2, $\psi_{\bar{\omega}}$ generates Π and thus has order n'. Since $N^*(\cdot)$ is cyclic of order $p^\lambda - 1$, n' is the least positive integer such that $l\alpha n'$ is a multiple of λ. Thus $\lambda/(l\alpha, \lambda) = n' = \lambda/l'$ and $l' = (l\alpha, \lambda)$.

Let $\lambda = \bar{l}\bar{n}$, where $\bar{l} = (l, \lambda)$. Thus $(l/\bar{l}, \bar{n}) = 1$ and $\bar{n}|n$, since $\lambda | ln$. Let $l = s\bar{l}$. Then $l' = \bar{l}(s\alpha, \bar{n})$. By Lemma 2.2 and the definition of I, $(\alpha, n) = (i, n) = (I, n)$. By Lemma 2.5, $(\alpha, \bar{n}) = (I, \bar{n})$, since $\bar{n}|n$. Hence, by Lemma 2.4, $l' = \bar{l}(sI, n) = (lI, \lambda)$ and the proof of the theorem is complete.

Now let $\lambda = lt$. It follows immediately from the sub-field structure of $K(+,\cdot)$ that N contains the centre of $K(+,\circ)$. Further, by Lemma 2.3, $I \equiv n/t \bmod n$ and $l' = (ln/t, lt) = l(n/t, t)$. Hence the corollary follows.

References

[1] L. E. Dickson, On finite algebras. Nachr. Akad. Wiss. Göttingen, Math.-Phys. Kl. II (1905) 358—393.

[2] E. Ellers und H. Karzel, Endliche Inzidenzgruppen. Abh. Math. Sem. Univ. Hamburg 27 (1964) 250—264.

[3] H. Karzel, Unendliche Dicksonsche Fastkörper. Arch. Math. (Basel) 16 (1965) 247—256.

[4] H. Zassenhaus, Über endliche Fastkörper. Abh. Math. Sem. Univ. Hamburg 11 (1936) 187—220.