BULL. AUSTRAL. MATH. SOC. MOS 12K05
VOL. 5 (1971), 275-280.

# The sub-near-field structure of finite near-fields

Susan Dancs

The sub-near-field structure of finite near-fields is analogous to the sub-field structure of finite fields. A finite near-field of order $p^{ln}$ contains a unique sub-near-field of order $p^{\lambda}$ if and only if $\lambda$ divides $ln$ .

## 1. Introduction

A (left distributive) near-field is a structure which satisfies all the axioms for a skew field except possibly right distributivity.

A pair of positive integers $q, n$ satisfying the 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 $n \not\equiv 0 \bmod 4$ ;

is called a Dickson number pair.

The results of Ellers and Karzel [2] and Zassenhaus [4] show that there is a uniform method for constructing a finite near-field of order $q^n$ , with centre of order $q$ , from the field of order $q^n$ , whenever $q, n$ is a Dickson number pair. The near-field obtained by this construction is called a Dickson near-field; $q$ and $n$ will be called its invariants. Moreover, with seven exceptions, all finite near-fields are Dickson. A list of the exceptional cases can be found on p. 391 of Hall [3].

Received 10 May 1971. Communicated by M.F. Newman. The author thanks Dr M.F. Newman for his help and encouragement with this work.



https://doi.org/10.1017/S000497270004716X Published online by Cambridge University Press

The results of this paper, together with those of [1], make it possible to describe completely the sub-near-field structure of finite near-fields.

For the exceptional cases this is easy. Each exceptional finite near-field has order $p^2$ and thus has precisely two sub-near-fields: the near-field itself and its prime field of order $p$ (which is not necessarily central).

Let $N$ be a sub-near-field of a finite Dickson near-field $K$, with invariants $q = p^l$, $n$. Since additively $N$ is a subgroup of $K$, the order $|N|$ of $N$ is $p^\lambda$, for some $\lambda$. Since multiplicatively $N^*$ is a subgroup of $K^*$, $p^\lambda - 1$ divides $p^{ln} - 1$ and hence $\lambda$ divides $ln$. It follows (Theorem of [1]) from the construction of $K$, that for every $\lambda$ dividing $ln$, there is a sub-near-field of $K$ of order $p^\lambda$, which is a Dickson near-field, with invariants $p^{l'}$, $\lambda/l'$, where $l'$ is the greatest common divisor of $lI$ and $\lambda$, and $I$ is the solution of $I \equiv \left(p^{ln}-1\right)/\left(p^\lambda-1\right) \bmod n$ such that $0 < I \leq n$.

In this paper the following result is proved.

THEOREM. *For each* $\lambda$ *dividing* $ln$, *a Dickson near-field of order* $p^{ln}$ *contains at most one sub-near-field of order* $p^\lambda$.

Thus an analogous result to that for finite fields has been obtained. A finite near-field of order $p^{ln}$ has a unique sub-near-field of order $p^\lambda$, if and only if $\lambda$ divides $ln$. Further, the structure of each sub-near-field can be completely specified.

## 2. Number-theoretic lemma

The proof of the theorem depends on the following number-theoretic result.

LEMMA 2.1. *Let* $g, h$ *be positive integers,* $h \neq 1$. *If every prime* $r$ *which divides* $p^{gh} - 1$ *also divides* $p^g - 1$, *then* $p$ *is a Mersenne prime,* $g = 1$ *and* $h = 2$.

Proof. It can readily be seen that, for all $k \geq 2$, there exists

https://doi.org/10.1017/S000497270004716X Published online by Cambridge University Press

$f \geq 1$ , such that

$$(*) \qquad p^{gk} - 1 = \left(p^g-1\right)\left[f\left(p^g-1\right)+k\right] .$$

Let $s$ be a prime divisor of $h$ , $w = \left(p^{gs}-1\right)/\left(p^g-1\right)$ and $r$ a prime divisor of $w$ . Then $r \mid p^{gs}-1$ and hence $r \mid p^{gh}-1$ . Thus, by assumption, $r \mid p^g-1$ . But $w = f\left(p^g-1\right) + s$ , for some $f$ . Hence $r \mid s$ and, consequently, $r = s$ . Thus $w = s^u$ with $u > 1$ , since both $f$ and $g$ are non-zero.

If $s$ is an odd prime, then

$$\begin{aligned} s^u = w &= 1 + p^g + \ldots + p^{g(s-1)} \\ &= \left(p^g-1\right)\left[s'\left(p^g-1\right) + \sum_{i=1}^{s-1} i\right] + s \text{ , by } (*), \\ &= \left(p^g-1\right)\left[s'\left(p^g-1\right)+s(s-1)/2\right] + s \\ &\equiv s \bmod s^2 \text{ , since } s \mid p^g-1 , \end{aligned}$$

contradicting $u > 1$ . Hence $s = 2$ , and $w = p^g + 1$ . Since $u > 1$ , it follows that $p^g \equiv 3 \bmod 4$ . Hence $p, g$ are odd. But then

$$2^u = p^g + 1 = (p+1)\left(p^{g-1}-p^{g-2} + \ldots - p+1\right)$$

implies $g = 1$ and $p$ is a Mersenne prime. Since $2$ is the only prime divisor of $h$ , $h = 2^v$ . If $v > 1$ , then $r \mid p^4-1$ would imply $r \mid p^h-1$ . But

$$\begin{aligned} \left(p^4-1\right)/(p-1) = \left(p^2+1\right)(p+1) &= \left(2^{2u}-2^{u+1}+2\right)2^u \\ &= 2^{u+1}\left[2^u\left(2^{u-1}-1\right)+1\right] , \end{aligned}$$

so $p^4 - 1$ would have an odd prime divisor dividing both $\left[2^u\left(2^{u-1}-1\right)+1\right]$ and $p - 1 = 2\left(2^{u-1}-1\right)$ , which is clearly impossible. Thus $v = 1$ , $h = 2$ .

## 3. Proof of the theorem

LEMMA 3.1 (Ellers und Karzel [2], Satz 1). *The multiplicative*

https://doi.org/10.1017/S000497270004716X Published online by Cambridge University Press

*group,* $K^*$ *, of a finite Dickson near-field of order* $q^n$ *, has two generators* $a$ *and* $b$ *which satisfy the following relations:*

(4) $a^m = 1$ , $b^n = a^t$ , $bab^{-1} = a^q$ ,

*where* $m, n, t$ *and* $q$ *satisfy the following conditions:*

(5) $m = (q^n-1)/n$ ;

(6) $t = m/(q-1)$ ;

(7) $q^n \equiv 1 \bmod m$ *and, if* $n > 1$ , $q^\nu \not\equiv 1 \bmod m$ *for* $1 \le \nu < n$ ;

(8) $(n, t) = (q-1, t) \le 2$ ;

(9) $(n, t) = (q-1, t) = 2$ *if and only if* $n \equiv 2 \bmod 4$ *and* $q \equiv 3 \bmod 4$ .

*Furthermore,* (*see* Hall [3], p. 390)

(10) *a Sylow subgroup of* $K^*$ *of odd order is cyclic. A Sylow* 2*-subgroup of* $K^*$ *is cyclic or generalized quaternion.*

For the remainder of this paper, $A$ will denote the normal subgroup of $K^*$ , of order $(p^{ln}-1)/n$ , generated by $a$ . Further, let $Z$ be the (unique) subgroup of $A$ of order $q - 1$ . Note $Z$ is the centre of $K^*$ .

LEMMA 3.2. *Let* $r$ *be a prime divisor of* $q - 1$ *and* $r^s$ *the highest power of* $r$ *dividing* $q - 1$ *. For all positive integers* $v \le s$ *, the group* $K^*$ *has a unique subgroup of order* $r^v$ .

Proof. Since $Z$ is normal in $K^*$ , the Sylow $r$-subgroup, $R$ , of $Z$ is contained in every Sylow $r$-subgroup, $S$ , of $K^*$ .

If $S$ is cyclic, the result follows. If $S$ is not cyclic, $r = 2$ and $(n, t) = 2$ . Then, by (9), $s = 1$ and $|R| = 2$ . But a generalized quaternion group has a unique subgroup of order 2 and, again, the result follows.

With these lemmas, the theorem can now be proved.

Let $N$ be a sub-near-field of $K$ , of order $p^\lambda$ , and $N^*$ the multiplicative group of $N$ .

https://doi.org/10.1017/S000497270004716X Published online by Cambridge University Press

Let $\bar{l} = (l, \lambda)$ and let $Z'$ be the (unique) subgroup of $Z$ of order $p^{\bar{l}} - 1$. Since $(p^{l}-1, p^{\lambda}-1) = (p^{\bar{l}}-1)$, $N^* \cap Z \le Z'$. Further, if $r^{\nu} | p^{\bar{l}} - 1$, for some prime $r$, then $r^{\nu} | p^{\lambda}-1$ and, by Lemma 3.2, $N^*$ contains a unique subgroup $R_{\nu}$, of order $r^{\nu}$. Hence $R_{\nu} \le Z'$ and so $|N^* \cap Z| = |Z'| = p^{\bar{l}} - 1$ and $N^* \cap Z = Z'$.

Hence $p^{\lambda} - 1 = (p^{\bar{l}}-1)t'n''$, where $|N^* \cap A| = (p^{\bar{l}}-1)t'$ and $n''|n$.

Let $M$ also be a sub-near-field of $K$, of order $p^{\lambda}$. Without loss of generality, it may be assumed that $|M^* \cap A| \ge |N^* \cap A|$. Since $(n, t) \le 2$, $|M^* \cap A|$ is $|N^* \cap A|$ or $2|N^* \cap A|$, and so $M^* \cap A \ge N^* \cap A$, since $A$ is cyclic. Therefore, $N^* \cap A \le (N \cap M)^* \le N^*$. Hence $|(N \cap M)^*| = (p^{\lambda}-1)/\mu$, where $\mu | n''$ and hence $\mu | n$.

But $N \cap M$ is a sub-near-field of $K$. Thus $(p^{\lambda}-1)/\mu = p^{\nu} - 1$, for some $\nu$. Further, since $N^* \cap Z \le (N \cap M)^* \le N^*$, $\bar{l} | \nu$ and $\nu | \lambda$.

If $r$ is a prime divisor of $p^{\lambda} - 1 = \mu(p^{\nu}-1)$, then either $r | p^{\nu}-1$ or $r | \mu$. If $r | \mu$, then $r | n$ and, by (2), $r | p^{l}-1$. Hence $r | p^{\bar{l}}-1$. So $r | p^{\nu}-1$.

Thus, by Lemma 2.1, either $\lambda = \nu$ and $N = M$, or $p$ is a Mersenne prime, $\lambda = 2$ and $\nu = 1$. If $p = 2^{u} - 1$, with $u > 1$, then $p \equiv 3 \bmod 4$. Further, since $1 = \bar{l} = (l, \lambda)$, $l$ is odd and $q \equiv 3 \bmod 4$. Since $\lambda | ln$, $n$ is even. Thus, by (3), $n \equiv 2 \bmod 4$. But $p^{\lambda} - 1 = p^{2} - 1 = (p-1)(p+1) = (p-1)2^{u}$. Thus $|N^* \cap A| \ge (p-1)2^{u-1}$, contradicting $|(N \cap M)^*| = p - 1$, since $u > 1$. Thus $N = M$ and the proof of the theorem is complete.

## References

[1] Susan Dancs, "On finite Dickson near fields", *Abh. Math. Sem. Univ. Hamburg* (submitted).

https://doi.org/10.1017/S000497270004716X Published online by Cambridge University Press

[2] Erich Ellers und Helmut Karzel, "Endliche Inzidenzgruppen", *Abh. Math. Sem. Univ. Hamburg* 27 (1964), 250-264.

[3] Marshall Hall, Jr, *The theory of groups* (The Macmillan Company, New York, 1959).

[4] Hans Zassenhaus, "Über endliche Fastkörper", *Abh. Math. Sem. Hansisch. Univ.* 11 (1936), 187-220.

Institute of Advanced Studies,
Australian National University,
Canberra, ACT.

https://doi.org/10.1017/S000497270004716X Published online by Cambridge University Press