

REDUCIBILITY OF TRANSLATES OF DICKSON POLYNOMIALS

GERHARD TURNWALD

(Communicated by William W. Adams)

ABSTRACT. Let K be a field and $a, b \in K$. The Dickson polynomial $D_n(x, a)$ is characterized by the equation $D_n(x + (a/x), a) = x^n + (a/x)^n$. We prove that $D_n(x, a) + b \in K[x]$ is reducible if and only if there is a prime $p|n$ such that $b = -D_p(c, a^{n/p})$ for some $c \in K$, or $n = 4k$ and $b = 4c^4 - 8a^k c^2 + 2a^{2k}$ for some $c \in K$. This result generalizes the well-known reducibility criterion for binomials; and it provides a reducibility criterion for $T_n(x) + c$ where $T_n(x)$ denotes the Chebyshev polynomial of degree n .

INTRODUCTION

Let K be a field. For every positive integer n and every $a \in K$ there is a unique polynomial $D_n(x, a) \in K[x]$ such that $D_n(x + (a/x), a) = x^n + (a/x)^n$. This polynomial is monic of degree n and the coefficients are polynomials in a independent of K (see 1.1). It is called the *Dickson polynomial* of degree n with parameter a . Note that $D_n(x, 0) = x^n$. The following theorem is the main result of the present paper. (See 2.5; cf. 2.4 and 2.6.)

Theorem. *The polynomial $D_n(x, a) + b \in K[x]$ is reducible iff there is a prime $p|n$ such that $b = -D_p(c, a^{n/p})$ for some $c \in K$, or $n = 4k$ and $b = 4c^4 - 8a^k c^2 + 2a^{2k}$.*

In the case $a = 0$ the above theorem yields the well-known description of reducible binomials (see 3.1). For finite fields (and $a \neq 0$) a reducibility criterion in terms of the order (in the multiplicative group of K) of a zero of $x^2 + bx + a^n$ was recently found by Gao and Mullen. In the final section we show how to deduce their theorem from our results. The final section also contains a very simple condition for the reducibility of $D_n(x, a)$. It turns out that the answer does not depend on a , provided that $a \neq 0$ and $n > 2$.

The Chebyshev polynomial $T_n(x)$ (usually defined by the property $T_n(\cos \varphi) = \cos n\varphi$) has integral coefficients and satisfies $T_n((x+x^{-1})/2) = (x^n + x^{-n})/2$. Hence $T_n(x)$ may be defined over every field K ; and $T_n(x) = D_n(2x, 1)/2$ if $\text{char}K \neq 2$. Thus, if $c \in K$ and $\text{char}K \neq 2$, $T_n(x) + c$ is reducible over K iff $D_n(x, 1) + 2c$ is reducible. In this situation the above theorem implies that $T_n(x) + c$ is reducible iff there is a prime $p|n$ such that $c = -T_p(d)$ for some $d \in K$, or $4|n$ and $c = 2d^4 - 4d^2 + 1$ for some $d \in K$.

Received by the editors September 10, 1996.

1991 *Mathematics Subject Classification.* Primary 12E10; Secondary 11T06.

Key words and phrases. Dickson polynomials, Chebyshev polynomials, binomials, reducibility.

The notation K will be reserved for fields. The multiplicative group and the characteristic of K are denoted by K^\times and $\text{char}K$, respectively; and \bar{K} denotes an algebraic closure of K . We always tacitly assume that k, m, n denote positive integers. For every m we write $K^{(m)} = \{a^m : a \in K\}$. For an extension field L of K of finite degree $[L : K]$ we let $N_{L/K}$ denote the norm map from L into K . The greatest common divisor of k and m will be denoted by (k, m) . An expression like $\gamma + a/\gamma$ is to be understood as $\gamma + (a/\gamma)$. We abbreviate ‘if and only if’ by ‘iff’.

1. PRELIMINARIES

1.1 *Remark.* The main theorem on symmetric polynomials shows that for every n there is a unique polynomial $D_n(x, y) \in \mathbf{Z}[x, y]$ such that $D_n(x + y, xy) = x^n + y^n$. Let K be a field and $a \in K$. Then $D_n(x, a) \in K[x]$ is characterized by the property $D_n(x + a/x, a) = x^n + (a/x)^n$. Moreover, it is clear that $D_n(x, a)$ is monic and has degree n . It follows that the Dickson polynomials (as described in the introduction) exist.

The defining property yields $D_1(x, a) = x$, $D_2(x, a) = x^2 - 2a$, and $D_n(x, a) = x D_{n-1}(x, a) - a D_{n-2}(x, a)$ if $n \geq 3$. Conversely, the Dickson polynomials can be defined recursively by this relation. One can prove that

$$D_n(x, a) = \sum_{k \leq n/2} \frac{n}{n-k} \binom{n-k}{k} (-a)^k x^{n-2k}.$$

This explicit formula is irrelevant for our purposes, however. (See [4] for more information on Dickson polynomials.)

1.2 **Lemma.** *The following properties hold for all $a \in K$ and all n .*

- (a) $D_2(x, a) = x^2 - 2a$, $D_4(x, a) = x^4 - 4ax^2 + 2a^2$.
- (b) $D_n(b + c, a) = b^n + c^n$ for all $b, c \in K$ with $bc = a$.
- (c) If n is odd (even) then $D_n(x, a)$ only contains odd (even) powers of x .
- (d) $D_{km}(x, a) = D_m(D_k(x, a), a^k)$ for all k, m .

Proof. Parts (a) and (c) are clear from the recurrence relation in 1.1, (b) follows from the definition, and (d) holds since both sides yield $x^{km} + (a/x)^{km}$ when x is replaced by $x + a/x$. □

1.3 **Lemma.** *Let $a, b \in K$.*

- (a) Let $\alpha \in \bar{K}$ be a zero of $D_m(x, a^k) + b$. Then $D_{km}(x, a) + b$ is reducible over K iff $D_m(x, a^k) + b$ is reducible over K or $D_k(x, a) - \alpha$ is reducible over $K(\alpha)$.
- (b) Let $m > 1$. Assume that $D_{2m}(x, a) + b$ is reducible over K and $D_m(x, a^2) + b$ is irreducible. Then $2a^m + (-1)^m b \in K^{(2)} \setminus \{0\}$.

Proof. (a) Let $\xi \in \bar{K}$ be a zero of $D_k(x, a) - \alpha$. From 1.2(d) we see that $D_{km}(\xi, a) + b = 0$. Hence $D_{km}(x, a) + b$ is reducible iff $[K(\xi) : K] < km$. The assertion easily follows by making use of the equality $[K(\xi) : K] = [K(\xi) : K(\alpha)][K(\alpha) : K]$.

(b) Let $\alpha \in \bar{K}$ be a zero of $D_m(x, a^2) + b$ and let $L = K(\alpha)$. From (a) we see that $D_2(x, a) - \alpha$ is reducible over L , i.e., $2a + \alpha \in L^{(2)}$. Thus $N_{L/K}(2a + \alpha) \in K^{(2)}$. Note that $2a + \alpha$ is a zero of the irreducible polynomial $f(x) = D_m(x - 2a, a^2) + b$. Hence $N_{L/K}(2a + \alpha) = (-1)^m f(0) \neq 0$. We have $D_m(-2a, a^2) = 2(-a)^m$ (by 1.2(b)) and hence $f(0) = 2(-a)^m + b$. Thus $2a^m + (-1)^m b = N_{L/K}(2a + \alpha) \in K^{(2)} \setminus \{0\}$. □

1.4 Lemma. *Let $\text{char}K \neq 2$, $a, b \in K$, and $f(x) = x^2 + ax + b$. Then $f(x^2)$ is reducible over K iff there exists $c \in K$ such that (i) $4b = a^2 - c^2$ or (ii) $4b = (a + c^2)^2$.*

In case (i) we have $f(x^2) = (x^2 + (a - c)/2)(x^2 + (a + c)/2)$ and in case (ii) we have $f(x^2) = (x^2 + cx + (a + c^2)/2)(x^2 - cx + (a + c^2)/2)$.

Proof. Assume that $f(x^2)$ is reducible. If $f(x)$ is reducible then $a^2 - 4b = c^2$ with $c \in K$. In the sequel we assume that $f(x)$ is irreducible. For every zero $\alpha \in \bar{K}$ of $f(x^2)$ we have $[K(\alpha) : K] = 2$ since $[K(\alpha^2) : K] = 2$ and $[K(\alpha) : K] < 4$. Hence $f(x^2) = g(x)h(x)$ where $g(x), h(x) \in K[x]$ are monic irreducible polynomials of degree 2. Let $g(x) = x^2 + cx + d$. If $g(x) = g(-x)$ then $c = 0$ and $-d$ is a zero of $f(x)$, a contradiction. Since $g(-x)$ is a monic irreducible factor of $f(x^2)$, we obtain $h(x) = g(-x)$ and thus $f(x^2) = x^4 + (2d - c^2)x^2 + d^2$. Hence $4b = (2d)^2 = (a + c^2)^2$. The converse is clear. \square

1.5 Lemma. *Let $a, b \in K$.*

(a) *Let $D_4(x, a) + b$ be reducible. Then $D_2(x, a^2) + b$ is reducible or $b = 4c^4 - 8ac^2 + 2a^2$ for some $c \in K$.*

(b) *Suppose that $b = 4c^4 - 8ac^2 + 2a^2$ for some $c \in K$. Then $D_4(x, a) + b = (x^2 - 2cx + 2(c^2 - a))(x^2 + 2cx + 2(c^2 - a))$ is reducible and $2a^2 + b \in K^{(2)}$; and $D_2(x, a^2) + b$ is irreducible iff $c \in K^\times$ and $2a - c^2 \notin K^{(2)}$.*

Proof. (a) Suppose that $D_2(x, a^2) + b$ is irreducible, i.e., $2a^2 - b \notin K^{(2)}$. It follows from 1.3(b) that $\text{char}K \neq 2$. Recall that $D_4(x, a) = x^4 - 4ax^2 + 2a^2$ (by 1.2(a)). The assertion is obtained by applying 1.4 to $f(x) = x^2 - 4ax + 2a^2 + b$.

(b) The first part holds since $2a^2 + b = 4(c^2 - a)^2$ and $D_4(x, a) + b = x^4 - 4ax^2 + 4(c^2 - a)^2$. The second part follows from $2a^2 - b = 4c^2(2a - c^2)$. (Note that $2a - c^2 \notin K^{(2)}$ implies that $\text{char}K \neq 2$.) \square

2. THE MAIN RESULTS

2.1 Proposition. *Let $a \in K^\times, b \in K$, and $n > 2$. Let $\beta \in \bar{K}$ be a zero of $x^2 + bx + a^n$.*

(a) *Let n be odd. Then $D_n(x, a) + b$ is reducible over K iff $x^n - \beta$ is reducible over $K(\beta)$.*

(b) *Assume that $\beta \in K$. Then $D_n(x, a) + b$ is reducible iff $x^n - \beta$ is reducible or $b^2 = 4a^n$.*

Proof. Let $\gamma \in \bar{K}$ be a zero of $x^n - \beta$, $\alpha = \gamma + a/\gamma$, and $L = K(\alpha)$. Note that $D_n(\alpha, a) = \beta + a^n/\beta = -b$. Hence $D_n(x, a) + b$ is reducible iff $[L : K] \neq n$.

(a) Let $n_1 = [K(\gamma) : K(\beta)]$ and $n_2 = [L : K]$. It remains to prove that $n_1 \neq n$ iff $n_2 \neq n$. We have $[K(\gamma) : K] = n_1 m_1$ with $m_1 = [K(\beta) : K] \leq 2$, and $[K(\gamma) : K] = m_2 n_2$ with $m_2 = [K(\gamma) : L] \leq 2$. The assertion follows since $n_1, n_2 \leq n$ and n is odd.

(b) Note that $b^2 = 4a^n$ holds iff $\beta = a^n/\beta$; $x^n - \beta$ is reducible iff $[K(\gamma) : K] \neq n$. We have $L \subseteq K(\gamma)$ and γ is a zero of $f(x) = (x - \gamma)(x - a/\gamma) \in L[x]$. If $\beta \neq a^n/\beta$ then γ and a/γ are not conjugate over L . In this case it follows that $\gamma \in L$ and $L = K(\gamma)$; and thus the assertion holds. Now suppose that $\beta = a^n/\beta$. Assume that $[L : K] = n$. Then it follows that $L = K(\gamma)$, $\gamma \neq a/\gamma$ (since $n > 2$), and $x^n - \beta$ is irreducible. Since a/γ is a zero of $x^n - \beta$, there exists a K -embedding $\sigma : K(\gamma) \rightarrow \bar{K}$ with $\sigma(\gamma) = a/\gamma$. Then $\sigma(\alpha) = \alpha$ and thus σ is trivial on L . Hence $L \neq K(\gamma)$ since $\sigma(\gamma) \neq \gamma$. This contradiction proves that $[L : K] \neq n$. The assertion follows. \square

2.2 Proposition. *Let $a, b \in K$. Let $\beta \in \bar{K}$ be a zero of $x^2 + bx + a^4$. Assume that $L = K(\beta) \neq K$ and $D_2(x, a^2) + b$ is irreducible.*

(a) *$D_4(x, a) + b$ is reducible iff there exists $\eta \in L$ such that $\beta = -4\eta^4$ and $2N_{L/K}(\eta) = a$.*

(b) *Suppose that $\zeta^2 = -1$, $\beta = -4\eta^4$, and $2a^2 + b = \varepsilon c^2$ with $\zeta, \eta \in L$, $\varepsilon = \pm 1$, and $c \in K$. Then $D_4(x, a) + b$ is reducible, $\zeta \in K$, and $-4 \in K^{(4)}$.*

Proof. (a) Suppose that $D_4(x, a) + b$ is reducible. By 1.5 there is $c \in K^\times$ such that $b = 4c^4 - 8ac^2 + 2a^2$ and $2a - c^2 \notin K^{(2)}$. It follows that $\text{char}K \neq 2$ and $c^2 \neq a$. Let $\xi = (\beta - a^2)/(a - c^2)$. Then $\xi \in L$, $\xi^2 = -4\beta$, and $\xi = (2a + \xi)^2/4c^2$. Hence $\beta = -4\eta^4$ with $\eta = (2a + \xi)/4c$. From $\xi^2 + 4(a - c^2)\xi + 4a^2 = 0$ we obtain $\eta^2 - c\eta + a/2 = 0$; and thus $N_{L/K}(\eta) = a/2$.

Conversely, suppose that $\beta = -4\eta^4$ and $N_{L/K}(\eta) = a/2$. Let σ denote the nontrivial K -automorphism of L . Then $c = \eta + \sigma(\eta) \in K$, $\eta\sigma(\eta) = a/2$, and $-b = \beta + \sigma(\beta)$. Hence $b/4 = \eta^4 + \sigma(\eta)^4 = D_4(c, a/2) = c^4 - 2ac^2 + a^2/2$ and $D_4(x, a) + b$ is reducible according to 1.5(b).

(b) Note that $c \neq 0$ since otherwise $\beta = a^2 \in K$. Let $\xi = (\beta - a^2)/c$. Then $\xi^2 = -\varepsilon\beta$ and $\xi^2 + \varepsilon c\xi + \varepsilon a^2 = 0$. We have $-4 = (2\xi)^2 = (1 + \zeta)^4$ and hence $\beta \in L^{(4)}$. Suppose that $\varepsilon = -1$. Then $\xi^2 \in L^{(4)}$ and hence $\xi \in L^{(2)}$ (since $-1 \in L^{(2)}$). Thus $-a^2 = N_{L/K}(\xi) \in K^{(2)}$ and $-1 \in K^{(2)}$. Hence without loss of generality we may restrict to the case $\varepsilon = 1$. Note that $\text{char}K \neq 2$ (since $\beta \neq 0$).

Assume that $\zeta \notin K$. Then there are $\lambda, \mu \in K$ such that $(\lambda + \mu\beta)^2 = -1$ and $\mu \neq 0$. It follows that $\beta^2 + 2\lambda\mu^{-1}\beta + (\lambda^2 + 1)/\mu^2 = 0$. Hence $2\lambda/\mu = b$, $(\lambda^2 + 1)/\mu^2 = a^4$, and $4a^4 - b^2 = 4/\mu^2 \in K^{(2)} \setminus \{0\}$. We obtain $2a^2 - b \in K^{(2)}$ since $2a^2 + b \in K^{(2)}$. This contradicts the irreducibility of $D_2(x, a^2) + b$. Thus we conclude that $\zeta \in K$.

From $\xi^2 = -\beta = 4\eta^4$ we get $\xi = \pm 2\eta^2$. Hence $a^2 = N_{L/K}(\xi) = 4N_{L/K}(\eta)^2$. It follows that $N_{L/K}(\eta) = \pm a/2$. Note that $N_{L/K}(\zeta) = \zeta^2$ and $N_{L/K}(\zeta\eta) = -N_{L/K}(\eta)$. Possibly replacing η by $\zeta\eta$, we may thus assume that $\beta = -4\eta^4$ and $N_{L/K}(\eta) = a/2$. Then $D_4(x, a) + b$ is reducible according to (a) and the proof is finished. \square

We will use the following part (for odd degree) of the well-known reducibility criterion for binomials (see 3.1). A proof may be found in [3, p.297], [5, p.662], and [7, p.91].

2.3 Lemma. *Let n be odd and $a \in K$. Then $x^n - a$ is reducible (over K) iff for some prime $p|n$ we have $a \in K^{(p)}$.*

2.4 Theorem. *Let $a, b \in K$. If $D_n(x, a) + b$ is irreducible then $D_m(x, a^{n/m}) + b$ is irreducible for every $m|n$. If $D_n(x, a) + b$ is reducible over K then $D_p(x, a^{n/p}) + b$ is reducible for some prime $p|n$, or $n = 4k$ and $D_4(x, a^k) + b$ is reducible.*

Proof. The first part holds by 1.3(a). By induction we may assume that the second part is valid (for all K and all $a, b \in K$) if n is replaced by $1, \dots, n - 1$. Suppose that $D_n(x, a) + b$ is reducible. First we assume that n is odd. If $a = 0$ then the assertion follows from 2.3 since $D_n(x, 0) = x^n$. If $a \neq 0$ then, according to 2.1(a), $x^n - \beta$ is reducible over $K(\beta)$ and we have to show that $x^p - \beta$ is reducible over $K(\beta)$ for some prime $p|n$. Again, the assertion follows by making use of 2.3.

In the sequel we suppose that $n = 2m$. The proof is finished if $D_2(x, a^m) + b$ is reducible. Thus we assume that $D_2(x, a^m) + b$ is irreducible. Let $\gamma \in \bar{K}$ be a zero

of $D_2(x, a^m) + b$ (i.e., $\gamma^2 = 2a^m - b$). From 1.3(a) we obtain that $D_m(x, a) - \gamma$ is reducible over $L = K(\gamma)$. By induction, $D_p(x, a^{m/p}) - \gamma$ is reducible over L for some prime $p|m$, or $4|m$ and $D_4(x, a^{m/4}) - \gamma$ is reducible over L .

If $2|m$ and $D_2(x, a^{m/2}) - \gamma$ is reducible then there are $\lambda, \mu \in K$ such that $2a^{m/2} + \gamma = (\lambda + \mu\gamma)^2$. We obtain $2a^{m/2} = \lambda^2 + (2a^m - b)\mu^2$ and $1 = 2\lambda\mu$. Thus $b = (\lambda^2 - 2a^{m/2})\mu^{-2} + 2a^m = 4\lambda^4 - 8a^{m/2}\lambda^2 + 2a^m$ and 1.5(b) implies that $D_4(x, a^{n/4}) + b$ is reducible.

Now suppose that p is an odd prime such that $p|m$ and $D_p(x, a^{m/p}) - \gamma$ is reducible over L . According to 1.3(a), $D_{2p}(x, a^{m/p}) + b$ is reducible over K . Hence 1.3(b) implies that $D_p(x, a^{n/p}) + b$ is reducible (since $2a^m - b \notin K^{(2)}$).

Finally we suppose that $4|m$, $D_4(x, a^{m/4}) - \gamma$ is reducible, and $D_2(x, a^{m/2}) - \gamma$ is irreducible over L . It follows from 1.3(b) that $2a^{m/2} - \gamma \in L^{(2)} \setminus \{0\}$. Note that $2a^{m/2} + \gamma \notin L^{(2)}$ (since $D_2(x, a^{m/2}) - \gamma$ is irreducible). Hence $2a^m + b = 4a^m - \gamma^2 \notin L^{(2)}$. Thus 1.3(b) yields that $D_m(x, a^2) + b$ is reducible and our assertion follows by induction. \square

2.5 Theorem. *Let $a, b \in K$ and n be a positive integer. Then $D_n(x, a) + b \in K[x]$ is reducible iff there is a prime $p|n$ such that $b = -D_p(c, a^{n/p})$ for some $c \in K$, or $n = 4k$ and $b = 4c^4 - 8a^k c^2 + 2a^{2k}$ for some $c \in K$.*

Proof. According to 2.4 and 1.5, we may restrict to the case where $n = p$ is a prime. We have to prove that the reducibility of $D_p(x, a) + b$ implies that there is a zero in K . The assertion is evident if $p = 2$. Thus we assume that p is odd. If $a = 0$ then 2.3 applies (since $D_p(x, 0) = x^p$). In the sequel we suppose $a \neq 0$. Choose $\beta \in \bar{K}$ such that $\beta^2 + b\beta + a^p = 0$. It follows from 2.1(a) that $x^p - \beta$ is reducible over $L = K(\beta)$. Hence (by 2.3) $\beta = \gamma^p$ for suitable $\gamma \in L$. From $D_p(\gamma + a/\gamma, a) = \beta + a^p/\beta = -b$ we see that it is sufficient to show that $\gamma + a/\gamma \in K$ for suitably chosen γ .

If $L = K$ then we are done. Hence we assume $L \neq K$. Then $[L : K] = 2$ and $N_{L/K}(\beta) = a^p$. From $N_{L/K}(\gamma)^p = N_{L/K}(\beta)$ we get $N_{L/K}(\gamma) = \zeta a$ where $\zeta \in K$ and $\zeta^p = 1$. Let $c = \zeta^{-(p+1)/2}$. Then $N_{L/K}(c) = c^2 = \zeta^{-1}$ and $N_{L/K}(c\gamma) = a$. Hence replacing γ by $c\gamma$ we may assume $N_{L/K}(\gamma) = a$ and then it follows that $\gamma + a/\gamma \in K$. \square

2.6 Remark. (a) The condition $b = 4c^4 - 8a^k c^2 + 2a^{2k}$ may be expressed in the form $b = D_4(\sqrt{2}c, a^k)$. In this case $D_4(x, a^k) + b$ is the product of $D_2(x - c, a^k) + c^2$ and $D_2(x + c, a^k) + c^2$ (cf. 1.5(b)).

(b) If $b = 4c^4 - 8a^k c^2 + 2a^{2k}$, then $2a^{2k} + b = 4(a^k - c^2)^2$ and $2a^{2k} - b = 4c^2(2a^k - c^2)$. If $D_2(x, a^{2k}) + b$ is irreducible then $2a^{2k} - b \notin K^{(2)}$ and hence $\text{char}K \neq 2$, $c \neq 0$, $2a^k - c^2 \notin K^{(2)}$, and $2a^{2k} + b \neq 0$ (since otherwise $2a^k - c^2 = c^2$). Thus these conditions may be added in the formulation of Theorem 2.5.

(c) The condition $b = 4c^4 - 8a^k c^2 + 2a^{2k}$ holds iff there is a square root $d \in K$ of $2a^{2k} + b$ such that $a^k + d/2 \in K^{(2)}$.

(d) Theorem 2.4 follows from 2.5.

3. SPECIAL CASES

The following result is well-known. It is sometimes called the Vahlen-Capelli theorem. For odd n it was quoted as Lemma 2.3.

3.1 Theorem. *Let $a \in K$. Then $x^n - a$ is reducible over K iff for some prime $p|n$ we have $a \in K^{(p)}$, or $4|n$ and $a \in -4K^{(4)}$.*

Proof. This follows from 2.5 since $D_n(x, 0) = x^n$. □

3.2 Theorem. *Let $n > 2$ and $a \in K^\times$. Then $D_n(x, a)$ is irreducible iff n is a power of 2 and $2 \notin K^{(2)}$.*

Proof. Suppose $D_n(x, a)$ is irreducible. If m is odd then (by 1.2(c)) $D_m(x, a^{n/m})$ is divisible by x . Hence 1.3(a) (or 2.5) shows that n is a power of 2 and $D_2(x, a^{n/2})$ is irreducible, i.e., $2a^{n/2} \notin K^{(2)}$. Thus $2 \notin K^{(2)}$. Conversely, suppose that n is a power of 2 and $2 \notin K^{(2)}$. Then $2a^{n/2} \notin K^{(2)}$ and hence 1.3(b) (or 2.5) implies that $D_4(x, a^{n/4})$ is irreducible. From 2.5 we conclude that $D_n(x, a)$ is irreducible. □

3.3 Remark. In the case $|K| < \infty$ the factorization of $D_n(x, a)$ has been found recently by Chou [1]. In the case where K is the field of rational numbers the factorization of Chebyshev polynomials is known (see [6, p.228]).

3.4 Lemma. *Let $|K| < \infty$ and $a, b \in K$. Let $\beta \in \bar{K}$ be a zero of $x^2 + bx + a^4$. Assume that $L = K(\beta) \neq K$. Then $D_4(x, a) + b$ is reducible iff $2a^2 - b \in K^{(2)}$ or $\beta \in L^{(4)}$.*

Proof. If q is even then $D_4(x, a) + b = x^4 + b$ is reducible and $L^{(4)} = L$. In the sequel we assume that q is odd. Note that $-1 \in L^{(2)}$. If $\zeta^2 = -1$ then $(1 + \zeta)^4 = -4$. Hence $-4 \in L^{(4)}$.

Let $D_4(x, a) + b$ be reducible. Then, according to 2.2(a), $D_2(x, a^2) + b$ is reducible or $\beta \in -4L^{(4)}$. Thus $2a^2 - b \in K^{(2)}$ or $\beta \in L^{(4)}$. Conversely, suppose that $2a^2 - b \in K^{(2)}$ or $\beta \in L^{(4)}$. If $2a^2 - b \in K^{(2)}$ then $D_2(x, a^2) + b$ is reducible and hence $D_4(x, a) + b$ is reducible (by 1.3(a)). Note that $b^2 - 4a^4 \notin K^{(2)}$ since $\beta \notin K$. Hence if $2a^2 - b \notin K^{(2)}$ then $-2a^2 - b \in K^{(2)}$, and then 2.2(b) implies that $D_4(x, a) + b$ is reducible since $\beta \in -4L^{(4)}$. □

3.5 Lemma. *Let $|K| = q < \infty$ and let e denote the order of $a \in K^\times$.*

- (a) $a \in K^{(m)}$ iff $(q - 1, m) \mid (q - 1)/e$.
- (b) Let p be a prime. Then $a \notin K^{(p)}$ iff $p \mid e$ and $p \nmid (q - 1)/e$.
- (c) Let $a \notin K^{(2)}$. Then $a \notin -4K^{(4)}$ iff $4 \mid q - 1$.

Proof. Part (a) is a simple consequence of the fact that K^\times is a cyclic group of order $q - 1$. Assertion (b) follows from (a) (since $e \mid q - 1$). Now let $a \notin K^{(2)}$. Note that q is odd. If $4 \nmid q - 1$ then $-1 \notin K^{(2)}$ and hence $-a/4 \in K^{(2)}$. From $(4, q - 1) = 2$ we obtain $K^{(2)} = K^{(4)}$ and hence $-a/4 \in K^{(4)}$. Conversely, $-a/4 \in K^{(4)}$ implies that $-1 \notin K^{(2)}$ and hence $4 \nmid q - 1$. Thus (c) is proved. □

The following result is, in a weaker form, due to Gao and Mullen [2]. (Remark 3.7 shows that their result follows from 3.6. In [2] it is also required that conditions similar to those given below hold for every e which is the order of a zero of $x^2 + bx + a^n$.)

3.6 Theorem. *Let $|K| = q < \infty$ and $n > 2$. Let $a \in K^\times$ and $b \in K$. Let e denote the order (in \bar{K}^\times) of some zero of $x^2 + bx + a^n$. Then $D_n(x, a) + b$ is irreducible iff the following conditions hold:*

- (i) Every odd prime factor of n divides e but does not divide $(q^2 - 1)/e$.
- (ii) If n is even and $e \mid q - 1$ then $b^2 \neq 4a^n$, $2 \mid e$, $2e \nmid q - 1$, and if $4 \mid n$ then $4 \mid q - 1$.
- (iii) If n is even and $e \nmid q - 1$ then $2a^{n/2} - b \notin K^{(2)}$, and if $4 \mid n$ then $4e \nmid q^2 - 1$.

Proof. If $e \mid q - 1$ then for every odd prime $p \mid e$ we have $(p, q + 1) = 1$. Hence in (i) we may replace $(q^2 - 1)/e$ by $(q - 1)/e$ if $e \mid q - 1$. Let $\beta \in \bar{K}$ be a zero of $x^2 + bx + a^n$ with order e . Note that $\beta \in K$ iff $e \mid q - 1$. Let $L = K(\beta)$.

First we suppose that n is odd. Then 2.1(a) shows that $D_n(x, a) + b$ is irreducible iff $x^n - \beta$ is irreducible over L . The latter condition holds (by 2.3) iff $\beta \notin L^{(p)}$ for every prime $p \mid n$. The assertion thus follows from 3.5(b).

Let $n = 2m$. If $e \mid q - 1$ then the assertion follows from 2.1(b) by making use of 3.1 and 3.5. In the sequel we assume that $e \nmid q - 1$. Note that $D_2(x, a^m) + b$ is irreducible iff $2a^m - b \notin K^{(2)}$. If $4 \nmid n$ then the assertion follows from 2.4 by making use of what we have already proved. If $4 \mid n$ then, in addition, we employ 3.4. The assertion follows since $2a^m - b \notin K^{(2)}$ implies that q is odd and hence $\beta \in L^{(4)}$ holds iff $e \mid (q^2 - 1)/4$ (by 3.5(a)). \square

3.7 Remark. We have $e \mid q^2 - 1$. If $e \mid q - 1$ then $b^2 - 4a^n \in K^{(2)}$. If $e \nmid q - 1$ then $b^2 - 4a^n \notin K^{(2)}$, or q is even and $b \neq 0$.

If (ii) or (iii) holds then q is odd. If (iii) holds then $b^2 - 4a^n \notin K^{(2)}$ and $2a^{n/2} - b \notin K^{(2)}$. Then it follows that $-2a^{n/2} - b = c^2$ with $c \in K^\times$ and hence from $\beta^2 + b\beta + a^n = 0$ we obtain $\beta = (\beta - a^{n/2})^2/c^2 \in L^{(2)}$. Thus (iii) implies that $2e \mid q^2 - 1$; and if $4 \mid n$ then it follows that $2 \mid e$ (since $4 \mid q^2 - 1$).

REFERENCES

- [1] W.-S. Chou: The factorization of Dickson polynomials over finite fields, *Finite Fields Appl.* **3** (1997), 84–96. CMP 97:07
- [2] S. Gao and G. L. Mullen: Dickson polynomials and irreducible polynomials over finite fields, *J. Number Theory* 49 (1994), 118–132. MR **95i**:11143
- [3] S. Lang: *Algebra* (Third Edition), Addison-Wesley, Reading, 1993.
- [4] R. Lidl, G. L. Mullen, and G. Turnwald: *Dickson Polynomials*, Pitman Monographs and Surveys in Pure and Applied Mathematics 65, Longman, Essex, 1993. MR **94i**:11097
- [5] L. Rédei: *Algebra*, Geest & Portig, Leipzig, 1959. (Pergamon Press, London, 1967.) MR **21**:4885; MR **35**:2697
- [6] T.J. Rivlin: *Chebyshev Polynomials* (Second Edition), Wiley, New York, 1990. MR **92a**:41016
- [7] A. Schinzel: *Selected Topics on Polynomials*, University of Michigan Press, Ann Arbor, 1982. MR **84k**:12010

MATHEMATISCHES INSTITUT, UNIVERSITÄT TüBINGEN, AUF DER MORGENSTELLE 10, D-72076 TüBINGEN, GERMANY

E-mail address: gerhard.turnwald@uni-tuebingen.de