

An explanation for the similar appearance of two identities involving Dickson polynomials

Antonia W. Bluer
National Security Agency
tbluer@access4less.net

February 20, 2022

Abstract

This article explains the similar appearance of two polynomial identities involving Dickson polynomials in char. 2, one found by Abhyankar, Cohen and Zieve, and the other found by the author.

1. Introduction

The k th Dickson polynomial $D_k(x) \in \mathbb{Z}[x]$ is defined by the recursion $D_k(x) = xD_{k-1}(x) - D_{k-2}(x)$ for $k \geq 2$, with the initial conditions $D_0(x) = 2$, $D_1(x) = x$. It satisfies the functional equation $D_k(u + 1/u) = u^k + u^{-k}$, which could serve as an alternate definition. If $k \geq 1$, then D_k is monic of degree k .

In [1], Abhyankar, Cohen, and Zieve found an identity of Dickson polynomials in finite characteristic, which in char. 2 may be written as follows, with $q = 2^n$:

$$X^{q^2-1} + (D_{q+1}(Y)/Y)X^{q-1} + Y^{q-1} = (X^{2q-2} + YX^{q-1} + 1) \left(\prod_{w \in \mathbb{F}_q^\times} (D_{q-1}(wX) - Y) \right). \quad (1)$$

In [2], the author found an identity that is special to char. 2:

$$X^{q^2-1} + (D_{q-1}(Y)/Y)X^{q-1} + Y^{q-1} = \prod_{w \in \mathbb{F}_q^\times} (D_{q+1}(wX) - Y). \quad (2)$$

It seems as though D_{q+1} and D_{q-1} switch roles in these equations. The identities were found independently, in different contexts, and with different applications, yet their visual similarity begs for an explanation. This article provides such an explanation.

We say a word about how the identities were found. The authors of [1] were motivated by some results in group theory which, when combined with Galois theory, led them to seek bivariate polynomials of a particular form with a particular type of factorization. This search led to them to discover the identity (1). The discovery of the second identity arose from the author's attempt to understand why certain pairs of polynomials in $\mathbb{F}_{2^n}[x]$ have related factorizations. The identity explained these related

factorizations and led to the result that if \mathbb{F} is any field of char. 2, $0 \neq a \in \mathbb{F}$, and $q = 2^n > 2$, then $x^{q+1} + x + 1/a$ and $C(x) + a$ have the same splitting field over \mathbb{F} , where $C(x) = x(\sum_{i=0}^{n-1} x^{2^i-1})^{q+1}$ is a Müller–Cohen–Matthews polynomial of degree $(q^2 - q)/2$.

Define $\langle u \rangle = u + 1/u$; then the Dickson relation may be written as $D_k(\langle u \rangle) = \langle u^k \rangle$. Note that

$$\begin{aligned} D_k \circ D_\ell(\langle u \rangle) &= D_k(\langle u^\ell \rangle) = \langle u^{\ell k} \rangle = D_{k\ell}(\langle u \rangle), \\ \langle u \rangle \langle v \rangle &= \langle uv \rangle + \langle u/v \rangle. \end{aligned} \tag{3}$$

These imply the well-known formulas:

$$D_k \circ D_\ell(x) = D_\ell \circ D_k(x) = D_{k\ell}(x), \quad D_k(x)D_\ell(x) = D_{k+\ell}(x) + D_{|k-\ell|}(x).$$

Let X be a transcendental over a field of char. 2, $q = 2^n$, and

$$v = D_{q-1}(X), \quad y = D_{q+1}(X), \quad z = D_{q^2-1}(X).$$

Let U be a solution to $U^2 + UX + 1 = 0$, so U is transcendental and

$$X = \langle U \rangle, \quad v = \langle U^{q-1} \rangle, \quad y = \langle U^{q+1} \rangle, \quad z = \langle U^{q^2-1} \rangle. \tag{4}$$

By (3), $\langle U^q \rangle \langle U \rangle = \langle U^{q+1} \rangle + \langle U^{q-1} \rangle$. Since $\langle U^q \rangle = \langle U \rangle^q$ in char. 2,

$$y + v = X^{q+1}. \tag{5}$$

The right side of (1) vanishes when one specializes $Y = v$, and so (1) implies

$$X^{q^2-1} + (D_{q+1}(v)/v)X^{q-1} + v^{q-1} = 0.$$

Likewise, the right side of (2) vanishes when one specializes $Y = y$, and so (2) implies

$$X^{q^2-1} + (D_{q-1}(y)/y)X^{q-1} + y^{q-1} = 0.$$

Now $D_{q+1}(v) = D_{q+1} \circ D_{q-1}(X) = D_{q^2-1}(X) = z$, and similarly $D_{q-1}(y) = z$. Thus, the above two formulas may be written as

$$X^{q^2-1} + (z/v)X^{q-1} + v^{q-1} = 0, \quad X^{q^2-1} + (z/y)X^{q-1} + y^{q-1} = 0.$$

Equivalently,

$$vX^{q^2} + zX^q + v^qX = 0, \tag{6}$$

$$yX^{q^2} + zX^q + y^qX = 0. \tag{7}$$

We showed that (1) implies (6) and (2) implies (7), but in fact (6) and (7) are easy to prove directly. Indeed, (6) follows from the calculation:

$$\begin{aligned} vX^{q^2} + zX^q + v^qX &= \langle U^{q-1} \rangle \langle U^{q^2} \rangle + \langle U^{q^2-1} \rangle \langle U^q \rangle + \langle U^{q(q-1)} \rangle \langle U \rangle \\ &= (\langle U^{q^2+q-1} \rangle + \langle U^{q^2-q+1} \rangle) + (\langle U^{q^2+q-1} \rangle + \langle U^{q^2-q-1} \rangle) + \\ &\quad (\langle U^{q^2-q+1} \rangle + \langle U^{q^2-q-1} \rangle) \qquad \text{by (3)} \\ &= 0 \end{aligned}$$

and (7) can be proved similarly. The sum of (6) and (7) is $(v+y)X^{q^2} + (v+y)^qX = 0$, which is consistent with the well-known formula (5).

2. Derivation of the identities

We showed that (1) easily implies (6), and (6) has a one-line proof. Similarly, (2) easily implies (7), and (7) has a one-line proof. Finally, we showed that (6) and (7) are related by the well-known formula (5). To complete the circle of ideas, we will show that (1) can be derived from the known formula (6) and (2) can be derived from the known formula (7). Much of the reasoning given in this section, as well as the one-line proofs of (6) and (7) from the previous section, can be found in the original proofs of the two polynomial identities; see [1, 2]. The new idea is simply to show how the similar appearance of (6) and (7) gives rise to the similar appearance of the two identities.

For most of the article, q denotes a power of 2, but in the next lemma q can be any prime power. If \mathbb{F} is a field, then $\overline{\mathbb{F}}$ denotes its algebraic closure.

Lemma 2.1 *Let \mathbb{K} be a field containing \mathbb{F}_q , $f, g \in \mathbb{K}[X]$, and $F(X) = f(X^{q-1})$. Suppose that $G(X) = \prod_{w \in \mathbb{F}_q^\times} g(wX)$ has no repeated roots in $\overline{\mathbb{K}}$. If every root of g in $\overline{\mathbb{K}}$ is also a root of F , then G divides F .*

Proof. Let $r \in \overline{\mathbb{K}}$ be any root of G . Then $g(wr) = 0$ for some $w \in \mathbb{F}_q^\times$, i.e., $s = wr$ is a root of g . By hypothesis, $F(s) = 0$. Then $F(r) = f((s/w)^{q-1}) = f(s^{q-1}) = F(s) = 0$. We have shown that every root of G in $\overline{\mathbb{K}}$ is also a root of $F(X)$. Since G has no repeated roots, G divides F . ■

Lemma 2.2 *Let $\mathbb{K} = \mathbb{F}_q(Y)$, where Y is transcendental and $q = 2^n$. If $k > 0$ is odd, then the polynomial $G(X) = \prod_{w \in \mathbb{F}_q^\times} (D_k(wX) - Y) \in \mathbb{K}[X]$ has no repeated roots in $\overline{\mathbb{K}}$.*

Proof. Let $x \in \overline{\mathbb{K}}$ be a root of $D_k(X) - Y$. Write $x = \langle u \rangle$, where $u \in \overline{\mathbb{K}}$. Then $Y = \langle u^k \rangle$. Since Y is transcendental over $\overline{\mathbb{F}}_q$, so is u . Let μ_k denote the k th roots of unity in $\overline{\mathbb{F}}_q$. Note that $|\mu_k| = k$ since k is prime to the characteristic. If $\zeta \in \mu_k$, then $D_k(\langle \zeta u \rangle) = \langle (\zeta u)^k \rangle = \langle u^k \rangle = Y$. Thus, $\langle \zeta u \rangle$ for $\zeta \in \mu_k$ are roots of $D_k(X) - Y$, and

$$\{ w \langle \zeta u \rangle : w \in \mathbb{F}_q^\times, \zeta \in \mu_k \} \text{ are roots of } G(X).$$

We claim these are distinct. To see this, suppose $w_1 \langle \zeta_1 u \rangle = w_2 \langle \zeta_2 u \rangle$. Then $(w_1 \zeta_1 + w_2 \zeta_2)u + (w_1/\zeta_1 + w_2/\zeta_2)u^{-1} = 0$. Since u is transcendental, both coefficients are zero, therefore $w_1 \zeta_1 + w_2 \zeta_2 = 0$, $w_1 \zeta_2 + w_2 \zeta_1 = 0$. On summing, we find $(w_1 + w_2)(\zeta_1 + \zeta_2) = 0$, so $w_1 = w_2$ or $\zeta_1 = \zeta_2$. If $w_1 = w_2$, then the equation $w_1 \zeta_1 + w_2 \zeta_2 = 0$ implies $\zeta_1 = \zeta_2$. If $\zeta_1 = \zeta_2$, then the same equation shows $w_1 = w_2$. This proves the claim. Since there are $(q-1)k$ distinct roots $w \langle \zeta u \rangle$ and $\deg_X(G) = (q-1)k$, they account for all the roots of G , therefore G has distinct roots. ■

Proof of the identity (2). Set $F(X) = X^{q^2-1} + (D_{q-1}(Y)/Y)X^{q-1} + Y^{q-1}$ and $g(X) = D_{q+1}(X) - Y$, considered as polynomials in $\mathbb{K}[X]$ where $\mathbb{K} = \mathbb{F}_q(Y)$. Let $x \in \overline{\mathbb{K}}$ be any root of g and write $x = \langle u \rangle$, where $u \in \overline{\mathbb{K}}$. Then $Y = \langle u^{q+1} \rangle$. Since Y is transcendental, so is u . In (4), replace U by u ; then $X = \langle U \rangle$, $y = \langle U^{q+1} \rangle$, and $z = \langle U^{q^2-1} \rangle$ are replaced by $x = \langle u \rangle$, $Y = \langle u^{q+1} \rangle$, and $D_{q-1}(Y) = \langle u^{q^2-1} \rangle$. Eq. (7) becomes $YxF(x) = 0$, so $F(x) = 0$. This shows that every root of g is a root of $F(X)$. By Lemmas 2.1 and 2.2, $\prod_{w \in \mathbb{F}_q^\times} g(wX)$ divides $F(X)$. Both polynomials are monic in X of degree $q^2 - 1$ and one divides the other, so they are equal. This proves (2). ■

Proof of the identity (1). Let X and V be independent transcendentals over \mathbb{F}_q . We will prove the identity (1) with Y replaced by V . Let $\mathbb{K} = \mathbb{F}_q(V)$ and define

$$F(X) = X^{q^2-1} + (D_{q+1}(V)/V)X^{q-1} + V^{q-1}, \quad G(X) = \prod_{w \in \mathbb{F}_q^\times} (D_{q-1}(wX) - V)$$

considered as elements of $\mathbb{K}[X]$. Let $x \in \overline{\mathbb{K}}$ be a root of $D_{q-1}(X) - V$ and write $x = \langle u \rangle$, where $u \in \overline{\mathbb{K}}$. Then $V = \langle u^{q-1} \rangle$. Since V is transcendental, so is u . In (4), replace U by u ; then $X = \langle U \rangle$, $v = \langle U^{q-1} \rangle$, and $z = \langle U^{q^2-1} \rangle$ are replaced by $x = \langle u \rangle$, $V = \langle u^{q-1} \rangle$, and $D_{q+1}(V) = \langle u^{q^2-1} \rangle$. Eq. (6) becomes $Vx F(x) = 0$, so $F(x) = 0$. This shows that every root of $D_{q-1}(X) - V$ is a root of $F(X)$. By Lemmas 2.1 and 2.2, G divides F .

Let $H(X) = F(X)/G(X) \in \mathbb{K}[X]$. Then $\deg_X(H) = (q^2 - 1) - (q - 1)^2 = 2(q - 1)$. Since $F(X)$ and $G(X)$ are monic, so is $H(X)$. We claim $H = h$, where

$$h(X) = X^{2q-2} + VX^{q-1} + 1.$$

Since H and h are monic of the same degree, it suffices to show that the roots of h in $\overline{\mathbb{K}}$ are distinct and that $h(r) = 0$ implies $G(r) \neq 0$ and $F(r) = 0$.

If h had a repeated root r , then $h(r) = h'(r) = 0$. Here, $h'(r) = Vr^{q-2}$ vanishes only at $r = 0$, but $h(0) \neq 0$. Thus, h has no repeated roots.

Next, $h(r) = 0$ if and only if $V = (r^{2q-2} + 1)/r^{q-1} = \langle r^{q-1} \rangle$. Since V is transcendental, so is r . For each $w \in \mathbb{F}_q^\times$, $D_{q-1}(wr) - V = D_{q-1}(wr) - \langle r^{q-1} \rangle$, and the right side is nonzero since $r^{q-1}(D_{q-1}(wx) - \langle r^{q-1} \rangle)$ is a nontrivial polynomial in $\mathbb{F}_q[r]$ and r is transcendental. This shows $G(r) \neq 0$.

Finally, since $D_{q+1}(V) = D_{q+1}(\langle r^{q^2-1} \rangle) = \langle r^{q^2-1} \rangle$,

$$\begin{aligned} VF(r) &= V r^{q^2-1} + D_{q+1}(V) r^{q-1} + V^q \\ &= \langle r^{q-1} \rangle r^{q^2-1} + \langle r^{q^2-1} \rangle r^{q-1} + \langle r^{q(q-1)} \rangle \\ &= (r^{q^2+q-2} + r^{q^2-q}) + (r^{q^2+q-2} + r^{q-q^2}) + (r^{q^2-q} + r^{q-q^2}) \\ &= 0. \end{aligned}$$

This shows $F(r) = 0$. The roots of h provide $2q - 2$ distinct roots of $H = F(X)/G(X)$, therefore $h = H$ and $F(X) = h(X)G(X)$. This proves (1). \blacksquare

References

- [1] Shereem S. Abhyankar, Stephen D. Cohen, and Michael E. Zieve, *Bivariate factorizations connecting Dickson polynomials and Galois theory*, Transactions of the American Mathematical Society **352**, No. 6, (2000), 2871–2887, doi: 10.1090/s0002-9947-00-02271-6.
- [2] Antonia W. Bluhner, *A new identity of Dickson polynomials*, to appear in Finite Fields and Their Applications.