TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 352, Number 6, Pages 2871–2887
S 0002-9947(00)02271-6
Article electronically published on February 28, 2000

BIVARIATE FACTORIZATIONS CONNECTING DICKSON POLYNOMIALS AND GALOIS THEORY

SHREERAM S. ABHYANKAR, STEPHEN D. COHEN, AND MICHAEL E. ZIEVE

Abstract. In his Ph.D. Thesis of 1897, Dickson introduced certain permutation polynomials whose Galois groups are essentially the dihedral groups. These are now called Dickson polynomials of the first kind, to distinguish them from their variations introduced by Schur in 1923, which are now called Dickson polynomials of the second kind. In the last few decades there have been extensive investigations of both of these types, which are related to the classical Chebyshev polynomials. We give new bivariate factorizations involving both types of Dickson polynomials. These factorizations demonstrate certain isomorphisms between dihedral groups and orthogonal groups, and lead to the construction of explicit equations with orthogonal groups as Galois groups.

1. Introduction

By the quadratic equation case of Newton's Theorem on symmetric functions we have the polynomial identity in indeterminates U_1 and U_2 given by

$$U_1^n + U_2^n = D_n(U_1 + U_2, U_1U_2) \quad \text{for } n \geq 0, \tag{1.1}$$

where $D_n(X, a)$ is a bivariate polynomial with integer coefficients. This is the most natural definition of the Dickson polynomial $D_n(X, a)$ of first kind, which was introduced by Dickson in [Di1]. This definition yields the recurrence relation

$$\begin{cases} D_{n+2}(X, a) = XD_{n+1}(X, a) - aD_n(X, a) & \text{for } n \geq 0 \\ \text{with initial conditions } D_0(X, a) = 2 \text{ and } D_1(X, a) = X, \end{cases} \tag{1.2}$$

which may also be taken as a definition of $D_n(X, a)$. By induction on n, from (1.2) we deduce the facts that

(1.3)

$$\begin{cases} D_n(X, a) \text{ is monic of degree } n \text{ in } X \text{ for } n \geq 1 \\ \text{and} \\ D_{2n}(X, a) = \widehat{D}_n(X^2, a) \text{ with polynomial } \widehat{D}_n(X, a) \text{ of degree } n \text{ in } X \text{ for } n \geq 0. \end{cases}$$

Received by the editors July 3, 1997 and, in revised form, November 21, 1997.

1991 *Mathematics Subject Classification.* Primary 12E05, 12F10, 14H30, 20D06, 20G40, 20E22.

Abhyankar's work was partly supported by NSF grant DMS 91-01424 and NSA grant MDA 904-97-1-0010. Zieve's work was partly supported by an NSF postdoctoral fellowship. Abhyankar and Zieve were also supported by EPSRC Visiting Fellowship GR/L 43329.

By induction on n, from (1.2) we deduce special formulas for some coefficients of $D_n(X,a)$, saying that

$$\begin{cases} \text{coeff of } X^{n-2[n/2]} \text{ in } D_n(X,a) = (-a)^{[n/2]}2 & \text{for even } n \geq 0 \\ \text{and} \\ \text{coeff of } X^{n-2[n/2]} \text{ in } D_n(X,a) = (-a)^{[n/2]}n & \text{for odd } n \geq 1 \\ \text{and} \\ \text{coeff of } X^{n-2} \text{ in } D_n(X,a) = -an & \text{for } n \geq 2, \end{cases} \tag{1.4}$$

where

$$[n/2] \text{ denotes the largest integer } \leq n/2.$$

More generally, by induction on n, from (1.2) we deduce the entire explicit formula

$$D_n(X,a) = \sum_{i=0}^{[n/2]} \frac{n}{n-i}\binom{n-i}{i}(-a)^i X^{n-2i} \quad \text{for } n \geq 1. \tag{1.5}$$

By putting $U_1 = U$ and $U_2 = \frac{a}{U}$ in (1.1), where U is another indeterminate, we get the functional equation

$$D_n(U + \frac{a}{U}, a) = U^n + \Big(\frac{a}{U}\Big)^n \quad \text{for } n \geq 0, \tag{1.6}$$

and from this we deduce the recurrence relations

$$D_m(X,a)D_n(X,a) = D_{m+n}(X,a) + a^n D_{m-n}(X,a) \quad \text{for } m \geq n \geq 0 \tag{1.7}$$

and

$$D_{mn}(X,a) = D_m(D_n(X,a), a^n) \quad \text{for } m \geq 0 \text{ and } n \geq 0 \tag{1.8}$$

and

$$D_n(bX, b^2a) = b^n D_n(X,a) \quad \text{for } n \geq 0 \tag{1.9}$$

where the last equation may be regarded as a trivariate identity. From (1.6) we also deduce the recurrence relations

$$\begin{cases} D_{2n}(X,a) = (D_n(X,a))^2 - 2a^n \quad \text{for } n \geq 0 \\ \text{and} \\ D_{2n+1}(X,a) = D_n(X,a)D_{n+1} - a^n X \quad \text{for } n \geq 0. \end{cases} \tag{1.10}$$

By the quadratic equation case of Newton's Theorem on symmetric functions we also have the polynomial identity in indeterminates U_1 and U_2 given by

$$\frac{U_1^{n+1} - U_2^{n+1}}{U_1 - U_2} = E_n(U_1 + U_2, U_1U_2) \quad \text{for } n \geq 0, \tag{1.11}$$

where $E_n(X,a)$ is a bivariate polynomial with integer coefficients. Again this is the most natural definition of the Dickson polynomial $E_n(X,a)$ of second kind, which was introduced by Schur in [Sch]. This definition yields the recurrence relation

$$\begin{cases} E_{n+2}(X,a) = XE_{n+1}(X,a) - aE_n(X,a) \quad \text{for } n \geq 0 \\ \text{with initial conditions } E_0(X,a) = 1 \text{ and } E_1(X,a) = X, \end{cases} \tag{1.12}$$

which may also be taken as a definition of $E_n(X,a)$. By induction on n, from (1.12) we deduce the facts that

(1.13)
$$\begin{cases} E_n(X,a) \text{ is monic of degree } n \text{ in } X \text{ for } n \geq 0 \\ \text{and} \\ E_{2n}(X,a) = \widehat{E}_n(X^2,a) \text{ with polynomial } \widehat{E}_n(X,a) \text{ of degree } n \text{ in } X \text{ for } n \geq 0. \end{cases}$$

By induction on n, from (1.12) we deduce special formulas for some coefficients of $E_n(X,a)$, saying that

$$\begin{cases} \text{coeff of } X^{n-2[n/2]} \text{ in } E_n(X,a) = (-a)^{[n/2]} & \text{for even } n \geq 0 \\ \text{and} \\ \text{coeff of } X^{n-2[n/2]} \text{ in } E_n(X,a) = (-a)^{[n/2]}(n+1)/2 & \text{for odd } n \geq 1 \\ \text{and} \\ \text{coeff of } X^{n-2} \text{ in } E_n(X,a) = -a(n-1) & \text{for } n \geq 2. \end{cases} \tag{1.14}$$

More generally, by induction on n, from (1.12) we deduce the entire explicit formula

$$E_n(X,a) = \sum_{i=0}^{[n/2]} \binom{n-i}{i} (-a)^i X^{n-2i} \quad \text{for } n \geq 0. \tag{1.15}$$

By putting $U_1 = U$ and $U_2 = a/U$ in (1.11), we get the functional equation

$$E_n(U + \frac{a}{U}, a) = \frac{U^{n+1} - \left(\frac{a}{U}\right)^{n+1}}{U - \frac{a}{U}} \quad \text{for } n \geq 0, \tag{1.16}$$

and from this we deduce the recurrence relations

$$E_m(X,a)E_n(X,a) = \frac{D_{m+n+2}(X,a) - a^{n+1}D_{m-n}(X,a)}{X^2 - 4a} \quad \text{for } m \geq n \geq 0 \tag{1.17}$$

and

$$E_m(D_n(X,a), a^n) = \frac{E_{mn+n-1}(X,a)}{E_{n-1}(X,a)} \quad \text{for } m \geq 0 \text{ and } n \geq 1 \tag{1.18}$$

and

$$E_n(bX, b^2a) = b^n E_n(X,a) \quad \text{for } n \geq 0. \tag{1.19}$$

Finally, by induction on n, from (1.2) and (1.12) we deduce the recurrence relations

$$\begin{cases} D_{n+2}(X,a) = XE_{n+1}(X,a) - 2aE_n(X,a) & \text{for } n \geq 0 \\ \text{and} \\ E_n(X,a) = -a^{[n/2]} + \sum_{i=0}^{[n/2]} a^i D_{n-2i}(X,a) & \text{for even } n \geq 0 \\ \text{and} \\ E_n(X,a) = \sum_{i=0}^{[n/2]} a^i D_{n-2i}(X,a) & \text{for odd } n \geq 1. \end{cases} \tag{1.20}$$

In Section 2 we shall review some more basic properties of Dickson polynomials, including their relationship with Chebyshev polynomials. Further discussion of Dickson polynomials can be found in the book [LMT] and in the papers [CM1] and [CM2].

Let $q > 1$ be a power of a prime p, let $k_p \subset \overline{k}_p$ be fields of characteristic p where $\overline{k}_p$ is an algebraic closure of k_p, and let k_q be the splitting field of $Y^q - Y$ over k_p in $\overline{k}_p$, i.e.,

$$k_q = k_p(\mathrm{GF}(q)) = \mathrm{SF}(Y^q - Y, k_p) \subset \overline{k}_p.$$

We shall now let a take various values in $\overline{k}_p$, and regard $E_n(X, a)$ and $D_n(Y, a)$ as members of the univariate polynomial rings $\overline{k}_p[X]$ and $\overline{k}_p[Y]$ respectively. In particular, let F be the monic polynomial of degree $1 + q$ in Y over $k_p[X]$ given by

$$F(X, Y) = Y^{1+q} - E_q(X, 1)Y + E_{q-1}(X, 1),$$

and let Φ and $\widehat{\Phi}$ be the monic polynomials of degree $q^2 - 1$ and q^2 in Y over $k_p[X]$ given by

$$\Phi(X, Y) = F(X, Y^{q-1}) = Y^{q^2-1} - E_q(X, 1)Y^{q-1} + E_{q-1}(X, 1)$$

and

$$\widehat{\Phi}(X, Y) = Y\Phi(X, Y) = Y^{q^2} - E_q(X, 1)Y^q + E_{q-1}(X, 1)Y.$$

In Section 3 we shall prove the following Factorization Theorem (1.T1) about the polynomials F and Φ, where $\overline{F}$ and F^* are the monic polynomials of degree 2 and $q - 1$ in Y over $k_p[X]$ given by

$$\overline{F}(X, Y) = Y^2 - XY + 1$$

and

$$F^*(X, Y) = \sum_{i=0}^{q-1} E_i(X, 1)Y^{q-1-i}$$

and $\overline{\Phi}$ and Φ^* are the monic polynomials of degree $2q - 2$ and $(q - 1)^2$ in Y over $k_p[X]$ given by

$$\overline{\Phi}(X, Y) = \overline{F}(X, Y^{q-1}) = Y^{2q-2} - XY^{q-1} + 1$$

and

$$\Phi^*(X, Y) = F^*(X, Y^{q-1}) = \sum_{i=0}^{q-1} E_i(X, 1)Y^{(q-1)(q-1-i)},$$

and where, as usual,

$$\mathrm{GF}(q)^* = \mathrm{GF}(q) \setminus \{0\}.$$

Factorization Theorem (1.T1). *In $k_p[X, Y]$ we have the factorizations*

$$F(X, Y) = \overline{F}(X, Y)F^*(X, Y) \quad \text{and} \quad \Phi(X, Y) = \overline{\Phi}(X, Y)\Phi^*(X, Y),$$

where $\overline{F}(X, Y)$ and $\overline{\Phi}(X, Y)$ are irreducible in $\overline{k}_p(X)[Y]$, and in $k_q[X, Y]$ we have the factorization

$$\Phi^*(X, Y) = \prod_{a \in GF(q)^*} [D_{q-1}(Y, a) - X]$$

of $\Phi^*(X, Y)$ into the $q - 1$ monic polynomials $D_{q-1}(Y, a) - X$ of degree $q - 1$ in Y over $k_q[X]$, each of which is irreducible in $\overline{k}_p(X)[Y]$. Moreover, if $p = 2$ then $F^*(X, Y)$ is irreducible in $\overline{k}_p(X)[Y]$.

In the case $p > 2$, in Section 3 we shall prove the following Supplementary Factorization Theorem (1.T2) about the polynomials F^* and Φ^*, where, for $1 \le j \le 2$, $F^{(j)}$ is the monic polynomial of degree $(q-1)/2$ in Y over $k_p[X]$ given by

$$F^{(j)}(X,Y) = \sum_{i=0}^{(q-1)/2} (-1)^i \binom{(q-1)/2}{i} E_{2i}((X+(-1)^j 2)^{1/2}, (-1)^j) Y^{(q-1-2i)/2}$$

and $\Phi^{(j)}$ is the monic polynomial of degree $(q-1)^2/2$ in Y over $k_p[X]$ given by

$$\begin{aligned}\Phi^{(j)}(X,Y) &= F^{(j)}(X, Y^{q-1}) \\ &= \sum_{i=0}^{(q-1)/2} (-1)^i \binom{(q-1)/2}{i} E_{2i}((X+(-1)^j 2)^{1/2}, (-1)^j) Y^{(q-1)(q-1-2i)/2}\end{aligned}$$

with

$$E_{2i}((X+(-1)^j 2)^{1/2}, (-1)^j) = \widehat{E}_i(X+(-1)^j 2, (-1)^j),$$

and where

$$\mathrm{GF}(q)^{(1)} = \begin{cases} \text{the set of all squares in } \mathrm{GF}(q)^* & \text{if } q \equiv 3 \pmod 4, \\ \text{the set of all nonsquares in } \mathrm{GF}(q)^* & \text{if } q \equiv 1 \pmod 4, \end{cases}$$

and

$$\mathrm{GF}(q)^{(2)} = \begin{cases} \text{the set of all squares in } \mathrm{GF}(q)^* & \text{if } q \equiv 1 \pmod 4, \\ \text{the set of all nonsquares in } \mathrm{GF}(q)^* & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

Supplementary Factorization Theorem (1.T2). *If $p > 2$, then in $k_p[X,Y]$ we have the factorizations*

$$F^*(X,Y) = F^{(1)}(X,Y)F^{(2)}(X,Y) \quad \text{and} \quad \Phi^*(X,Y) = \Phi^{(1)}(X,Y)\Phi^{(2)}(X,Y),$$

where $F^{(1)}(X,Y)$ and $F^{(2)}(X,Y)$ are irreducible in $\overline{k}_p(X)[Y]$, and in $k_q[X,Y]$ we have the factorization

$$\Phi^{(j)}(X,Y) = \prod_{a \in \mathrm{GF}(q)^{(j)}} [D_{q-1}(Y,a) - X] \quad \text{for } 1 \le j \le 2.$$

In Section 3 we shall also prove the following Normic Theorem (1.T3), which expresses the above polynomials Φ^* and $\Phi^{(j)}$ as the field theoretic norms $N_{k(X,Y^n)/k(X,Y^{mn})}(z)$ of certain elements $z \in k(X,Y^n)$ relative to the field extensions $k(X,Y^n)$ of $k(X,Y^{mn})$, where n and m are certain positive integers and k is any field between k_q and $\overline{k}_p$, and hence, in view of the above factorizations, provides alternative definitions of the above polynomials $F, \Phi, F^*, \Phi^*, F^{(j)}$, and $\Phi^{(j)}$.

Normic Theorem (1.T3). *If k is any field between k_q and $\overline{k}_p$ then, in the case $p = 2$, we have*

$$\Phi^*(X,Y) = N_{k(X,Y)/k(X,Y^{q-1})}(D_{q-1}(Y,1) - X),$$

and, in the case $p > 2$, for any $l_j \in GF(q)^{(j)}$ we have

$$\Phi^{(j)}(X,Y) = N_{k(X,Y^2)/k(X,Y^{q-1})}(D_{q-1}(Y,l_j) - X) \quad \text{for } 1 \le j \le 2,$$

where we note that we can always take $l_2 = -1$, and if $q-1$ is nondivisible by 4 we can also take $l_1 = 1$.

In Section 4 we shall relate Dickson polynomials with dihedral groups. In particular, we shall prove the following Dihedral Theorem (1.T4), where, as usual, by $\mathrm{Gal}(L,K)$ we denote the Galois group of a Galois extension L of a field K, and by $\mathrm{Gal}(f,K)$ we denote the Galois group of a univariate separable polynomial f over K, i.e., the Galois group of the splitting field of f over K regarded as a permutation group on the roots of f. Moreover, for every positive integer n, by Z_n we denote the cyclic group of order n, and by DL_{2n} we denote the dihedral group of order $2n$ which is defined as the semidirect product

$$DL_{2n} = Z_n \rtimes Z_2,$$

where the nonidentity element of Z_2 acts on Z_n by sending every element to its inverse. Via its regular representation, we may regard DL_{2n} as a subgroup of the symmetric group S_{2n} on $2n$ letters. We also define the modified dihedral group MDL_n as the subgroup of S_n generated by the "rotation" ρ given by $\rho(i) = i+1$ or 1 according as $1 \le i < n$ or $i = n$, and the "reflection" ρ' given by $\rho'(n) = n$ together with $\rho'(i') = n - i'$ for $1 \le i' \le n-1$. Note that then

$$MDL_n \approx \begin{cases} DL_{2n} & \text{if } n \ge 3, \\ Z_n & \text{if } 1 \le n \le 2, \end{cases}$$

where $\approx$ denotes isomorphism.

Dihedral Theorem (1.T4). *If a field k contains a primitive n-th root of 1, where n is a positive integer which is not divisible by the characteristic of k, then for any $0 \ne a \in k$ we have $\mathrm{Gal}(D_n(Y,a) - X, k(X)) = MDL_n$. Moreover, if k is a field between k_q and $\overline{k}_p$ and $n = q-1$ then we have the following:*

(1.T4.1) $\mathrm{Gal}(\overline{\Phi}, k(X)) = DL_{2n}$ *and* $\mathrm{Gal}(\overline{F}, k(X)) = S_2$*;*

(1.T4.2) $\mathrm{Gal}(F^*, k(X)) = MDL_n$ *for* $p = 2$*;*

(1.T4.3) $\mathrm{Gal}(F^*, k(X)) \approx \mathrm{Gal}(F^{(j)}, k(X)) = MDL_{n/2}$ *for* $p > 2 \ge j \ge 1$ *and* $q \ne 5$*; and*

(1.T4.4) $\mathrm{Gal}(F^*, k(X)) = DL_4$ *and* $\mathrm{Gal}(F^{(j)}, k(X)) = MDL_2$ *for* $2 \ge j \ge 1$ *and* $q = 5$.

In Section 5 we shall show how the above factorizations illustrate certain relationships between dihedral groups and orthogonal groups. In particular we shall prove the following Orthogonal Theorem (1.T5); for the basic theory of the orthogonal groups $\mathrm{O}^+(2m,q)$ and their projectivizations $\mathrm{PO}^+(2m,q)$ see the book [Di2] of Dickson or the book [KLi] of Kleidman and Liebeck; indeed, one of the starting points of our present investigation was Proposition (2.9.1)(iii) on page 43 of [KLi] stating that $\mathrm{O}^+(2,q) \approx DL_{2(q-1)}$, and hence $\mathrm{PO}^+(2,q) \approx DL_{2(q-1)}$ or DL_{q-1} according as $p = 2$ or $p > 2$.

Orthogonal Theorem (1.T5). *If k is any field between k_q and $\overline{k}_p$, then for the polynomials $\widehat{\Phi}$ and F we have $\mathrm{Gal}(\widehat{\Phi}, k(X)) = \mathrm{O}^+(2,q)$ and $\mathrm{Gal}(F, k(X)) = \mathrm{PO}^+(2,q)$.*

As noted in Theorem (b) of [Lie], in its action on the $2m-1$ dimensional projective space, $\mathrm{PO}^+(2m,q)$ has two orbits of sizes $(1+q+\cdots+q^{m-1})(q^{m-1}+1)$ and $q^{m-1}(q^m-1)$ in the case $p = 2$, and three orbits of sizes $(1+q+\cdots+q^{m-1})(q^{m-1}+1)$, $(1/2)q^{m-1}(q^m-1)$ and $(1/2)q^{m-1}(q^m-1)$ in the case $p > 2$. Although in [Lie] it is assumed that $m \ge 2$, these orbit sizes are valid also for $m = 1$. Thus, in its action on the projective line, the orbit sizes of $\mathrm{O}^+(2,q)$ are 2 and $q-1$ in the case $p = 2$,

and 2, $(1/2)(q-1)$ and $(1/2)(q-1)$ in the case $p > 2$. This is in accordance with the Y-degrees of the factors $\overline{F}$ and F^* of F in the case $p = 2$, and the factors $\overline{F}$, $F^{(1)}$ and $F^{(2)}$ of F in the case $p > 2$. This prediction of the degrees of the factors was the primary starting point of our present investigation, which consisted in a search for suitable polynomials F and Φ. All this becomes even more significant in the construction of equations with Galois groups $\mathrm{O}^+(2m, q)$ and $\mathrm{PO}^+(2m, q)$ for $m > 1$, which will be discussed elsewhere. For analogous construction of equations with the orthogonal groups $\mathrm{O}^-(2m, q)$ and $\mathrm{PO}^-(2m, q)$ as groups, see [Ab7]. Likewise, for the construction of equations with linear, unitary and symplectic groups see [Ab3], [Ab5] and [Ab6] respectively. Moreover, for an overview of the construction of equations see [Ab4] and [Ab8], and for algebro-geometric background see [Ab1] and [Ab2]. A review of all these groups can be found in the papers [Ab2]–[Ab8] as well as the books [Di2] and [KLi].

2. Remarks on the Algebra of Dickson Polynomials

In Remarks (2.1) to (2.4), we shall again regard $D_n(X, a)$ and $E_n(X, a)$ as bivariate polynomials with integer coefficients.

Remark 2.1. For $n \geq 1$ and another indeterminate Y, we get

$$\begin{aligned}(Y^2 - XY + 1)\sum_{i=0}^{n} D_i(X,1)Y^{n-i} &= D_0(X,1)Y^{n+2} + [D_1(X,1) - XD_0(X,1)]Y^{n+1} \\ &\quad - [XD_n(X,1) - D_{n-1}(X,1)]Y + D_n(X,1) \\ &\quad + \sum_{i=0}^{n-2}[D_{i+2}(X,1) - XD_{i+1}(X,1) + D_i(X,1)]Y^{n-i},\end{aligned}$$

and by (1.2) the RHS equals $2Y^{n+2} - XY^{n+1} - D_{n+1}(X,1)Y + D_n(X,1)$; hence

$$(2.1.1)\quad \begin{cases}\text{letting } \widetilde{D}_n(X,Y) = 2Y^{n+2} - XY^{n+1} - D_{n+1}(X,1)Y + D_n(X,1) \\ \text{we have } \widetilde{D}_n(X,Y) = (Y^2 - XY + 1)\sum_{i=0}^{n} D_i(X,1)Y^{n-i} \text{ for } n \geq 1.\end{cases}$$

For $n \geq 1$, we also get

$$\begin{aligned}(Y^2 - XY + 1)\sum_{i=0}^{n} E_i(X,1)Y^{n-i} &= E_0(X,1)Y^{n+2} + [E_1(X,1) - XE_0(X,1)]Y^{n+1} \\ &\quad - [XE_n(X,1) - E_{n-1}(X,1)]Y + E_n(X,1) \\ &\quad + \sum_{i=0}^{n-2}[E_{i+2}(X,1) - XE_{i+1}(X,1) + E_i(X,1)]Y^{n-i}\end{aligned}$$

and by (1.12) the RHS equals $Y^{n+2} - E_{n+1}(X,1)Y + E_n(X,1)$; hence

$$(2.1.2)\quad \begin{cases}\text{letting } \widetilde{E}_n(X,Y) = Y^{n+2} - E_{n+1}(X,1)Y + E_n(X,1) \\ \text{we have } \widetilde{E}_n(X,Y) = (Y^2 - XY + 1)\sum_{i=0}^{n} E_i(X,1)Y^{n-i} \text{ for } n \geq 1.\end{cases}$$

Remark 2.2. In the notation of (2.1.2), the fact that $Y^2 - XY + 1$ divides $\widetilde{E}_n(X,Y)$ as a polynomial in X and Y, i.e., equivalently, the fact that $Y - X + Y^{-1}$ divides $\widetilde{E}_n(X,Y)$ as a polynomial in X over the rational function field in Y, can also be

seen by noting that by (1.16) we have

$$\widetilde{E}_n(Y+Y^{-1},Y) = Y^{n+2} - \frac{(Y^{n+2}-Y^{-n-2})Y}{Y-Y^{-1}} + \frac{Y^{n+1}-Y^{-n-1}}{Y-Y^{-1}}$$

and, by cancelling like terms with opposite signs, the RHS equals zero, and hence

$$\widetilde{E}_n(Y+Y^{-1},Y) = 0. \tag{2.2.1}$$

Here, instead of using (1.16) we could use (1.6) and (1.20). Similarly, in the notation of (2.1.1), the fact that $Y^2 - XY + 1$ divides $\widetilde{D}_n(X,Y)$ as a polynomial in X and Y, i.e., equivalently, the fact that $Y - X + Y^{-1}$ divides $\widetilde{D}_n(X,Y)$ as a polynomial in X over the rational function field in Y, can be seen by noting that by (1.6) we have

$$\widetilde{D}_n(Y+Y^{-1},Y) = 0. \tag{2.2.2}$$

Remark 2.3. Although we shall not use it in this paper, to explain the relationship of the Dickson polynomials with the Chebyshev polynomials $T_n(X)$ and $U_n(X)$, respectively of first and second kind, we note that, over the complex field, for $n \geq 0$, these are defined by the trigonometric identities

$$\cos(n\Theta) = T_n(\cos\,\Theta) \quad \text{and} \quad \frac{\sin((n+1)\Theta)}{\sin\,\Theta} = U_n(\cos\,\Theta), \tag{2.3.1}$$

and, say by (1.2) and (1.12), we deduce that

$$D_n(X,1) = 2T_n(X/2) \quad \text{and} \quad E_n(X,1) = U_n(X/2). \tag{2.3.2}$$

Remark 2.4. Letting ξ be a primitive $(2n)$-th root of 1 and η be a primitive $(n+1)$-th root of 1, by putting $X = U + aU^{-1}$ in (1.6) and (1.16) we get the factorizations

$$D_n(X,a) = X^{n-2[n/2]} \prod_{i=1}^{[n/2]} [X^2 - (2 + \xi^{2i-1} + \xi^{2n-2i+1})a] \quad \text{for } n \geq 1 \tag{2.4.1}$$

and

$$E_n(X,a) = X^{n-2[n/2]} \prod_{i=1}^{[n/2]} [X^2 - (2 + \eta^i + \eta^{n+1-i})a] \quad \text{for } n \geq 0 \tag{2.4.2}$$

and

$$E_{2n-1}(X,a) = E_{n-1}(X,a)D_n(X,a) \quad \text{for } n \geq 1. \tag{2.4.3}$$

Remark 2.5. Recalling that k_p is a field of characteristic $p > 0$ and $q > 1$ is a power of p, and regarding $D_n(X,a)$ and $E_n(X,a)$ as members of $k_p[X]$ with $a \in k_p$, by (1.6) and (1.16) we get

$$D_q(X,a) = X^q \in k_p[X] \quad \text{for } a \in k_p \tag{2.5.1}$$

and

$$E_{q-1}(X,a) = \begin{cases} X^2 - 4a)^{(q-1)/2} \in k_p[X] & \text{for } q \text{ odd and } a \in k_p, \\ X^{q-1} & \text{for } q \text{ even and } a \in k_p, \end{cases} \tag{2.5.2}$$

where we note that these identities can also be deduced respectively from (2.4.1) and (2.4.2) by "reduction mod p." For use in the proof of Theorem (1.T2) to be given in Section 3, we note that by (1.4) we also have

$$D_{q-1}(0,a) = (-a)^{(q-1)/2}2 \quad \text{for } p > 2 \text{ and } 0 \neq a \in \mathrm{GF}(q),$$

and hence by (2.5.2) we get

$$E_{q-1}((D_{q-1}(0,a)+(-1)^j 2)^{1/2},(-1)^j) = [(-a)^{(q-1)/2}2 + (-1)^j 2 - (-1)^j 4]^{(q-1)/2} \quad \text{for } p > 2 \geq j \geq 1 \text{ and } 0 \neq a \in \mathrm{GF}(q),$$

and therefore

$$\text{(2.5.3)} \qquad \begin{cases} E_{q-1}((D_{q-1}(0,a)+(-1)^j 2)^{1/2},(-1)^j) \neq 0 \\ \text{for } p > 2 \geq j \geq 1 \text{ and } a \in \mathrm{GF}(q)^* \setminus \mathrm{GF}(q)^{(j)} \\ \text{with } \mathrm{GF}(q)^* \text{ and } \mathrm{GF}(q)^{(j)} \text{ as in Section 1.} \end{cases}$$

3. Factorizations

To prove Theorems (1.T1)–(1.T3), let the notation be as in Section 1.

For $a \in \mathrm{GF}(q)^*$, letting $n = q-1$, and letting $(\mu,\nu) = (1,0)$ or $(0,1)$ according as q is even or odd, successively by (2.5.1), (1.20), (1.8), and (1.7) we see that

$$\begin{aligned}
&\widehat{\Phi}(D_{q-1}(Y,a),Y) \\
&= D_{(n+1)(n+1)}(Y,a) - D_{n+1}(Y,a)E_{n+1}(D_n(Y,a),1) + D_1(Y,a)E_n(D_n(Y,a),1) \\
&= D_{(n+1)(n+1)}(Y,a) + \mu D_{n+1}(Y,a) - \nu D_1(Y,a) \\
&\quad - \left[D_{n+1}(Y,a)\sum_{i=0}^{[(n+1)/2]} D_{n+1-2i}(D_n(Y,a),1)\right] + \left[D_1(Y,a)\sum_{i=0}^{[n/2]} D_{n-2i}(D_n(Y,a),1)\right] \\
&= D_{(n+1)(n+1)}(Y,a) + \mu D_{n+1}(Y,a) - \nu D_1(Y,a) \\
&\quad - \left[D_{n+1}(Y,a)\sum_{i=0}^{[(n+1)/2]} D_{(n+1-2i)n}(Y,a)\right] + \left[D_1(Y,a)\sum_{i=0}^{[n/2]} D_{(n-2i)n}(Y,a)\right] \\
&= D_{(n+1)(n+1)}(Y,a) + \mu D_{n+1}(Y,a) - \nu D_1(Y,a) \\
&\quad - \left[\sum_{i=0}^{[(n+1)/2]} D_{(n+2-2i)n+1}(Y,a)\right] + \left[\sum_{i=0}^{[n/2]} D_{(n-2i)n+1}(Y,a)\right] \\
&\quad - a\left[\sum_{i=0}^{[(n+1)/2]-1} D_{(n-2i)n-1}(Y,a)\right] - \nu D_1(Y,a) - \mu D_{n+1}(Y,a) \\
&\quad + a\left[\sum_{i=0}^{[n/2]-\nu} D_{(n-2i)n-1}(Y,a)\right] + \nu D_1(Y,a) \\
&= 0,
\end{aligned}$$

where the last equality follows by cancelling like terms with opposite signs. Alternatively, for $a \in \mathrm{GF}(q)^*$, by putting $Y = U + aU^{-1}$, successively by (1.6) and

(1.16) we get

$$\begin{aligned}
&\widehat{\Phi}(D_{q-1}(Y,a),Y)\\
&= (u^{q^2}+au^{-q^2})-(u^q+au^{-q})e_q(u^{q-1}+u^{1-q},1)+(U+aU^{-1})E_{q-1}(U^{q-1}+U^{1-q},1)\\
&= \frac{(U^{q^2}+aU^{-q^2})(U^{q-1}-U^{1-q})}{U^{q-1}-U^{1-q}}\\
&\quad - \frac{(U^q+aU^{-q})(U^{q^2-1}-U^{1-q^2})}{U^{q-1}-U^{1-q}} + \frac{(U+aU^{-1})(U^{q^2-q}-U^{q-q^2})}{U^{q-1}-U^{1-q}}\\
&= 0,
\end{aligned}$$

where the last equality follows by cancelling like terms with opposite signs. Thus we have given two proofs of the fact that

$$\widehat{\Phi}(D_{q-1}(Y,a),Y) = 0 \quad \text{for all } a \in \mathrm{GF}(q)^*. \tag{3.1}$$

If $p > 2$, then, putting $X = U^2 + U^{-2}$ so that $(X + (-1)^j 2)^{1/2} = U + (-1)^j U^{-1}$ for $1 \le j \le 2$, by (1.16) we get

$$F^*(X,Y) = \sum_{i=0}^{q-1} \frac{(U^{2i+2} - U^{-2-2i})Y^{q-1-i}}{U^2 - U^{-2}}$$

and

$$\prod_{j=1}^{2} F^{(j)}(X,Y) = \prod_{j=1}^{2} \left[\sum_{i=0}^{(q-1)/2} \frac{(-1)^i \binom{(q-1)/2}{i} \left(U^{2i+1} - (-1)^j U^{-1-2i}\right) Y^{(q-1-2i)/2}}{U - (-1)^j U^{-1}} \right]$$

and by rearranging terms we see that

$$\begin{aligned}
&\text{the RHS of the above equation for } F^*(X,Y)\\
&= \frac{\left(U^2 \sum_{i=0}^{q-1} U^{2i} Y^{q-1-i}\right) - \left(U^{-2} \sum_{i=0}^{q-1} U^{-2i} Y^{q-1-i}\right)}{U^2 - U^{-2}}\\
&= \frac{U^2(Y-U^2)^{q-1} - U^{-2}(Y-U^{-2})^{q-1}}{U^2 - U^{-2}}\\
&= \prod_{j=1}^{2} \left[\frac{U(Y-U^2)^{(q-1)/2} - (-1)^j U^{-1}(Y-U^{-2})^{(q-1)/2}}{U - (-1)^j U^{-1}} \right]\\
&= \text{the RHS of the above equation for } \prod_{j=1}^{2} F^{(j)}(X,Y),
\end{aligned}$$

where the second and third equalities follow by using the identities $(A-B)^{q-1} = \sum_{i=0}^{q-1} B^i A^{q-1-i}$ and $A^2 - B^2 = \prod_{j=1}^{2}[A - (-1)^j B]$ respectively, and the fourth equality follows by using the binomial theorem. Thus

$$F^*(X,Y) = F^{(1)}(X,Y)F^{(2)}(X,Y) \quad \text{if } p > 2, \tag{3.2}$$

and hence

$$\Phi^*(X,Y) = \Phi^{(1)}(X,Y)\Phi^{(2)}(X,Y) \quad \text{if } p > 2. \tag{3.3}$$

By (2.1.2) we have

$$F(X,Y) = \overline{F}(X,Y)F^*(X,Y), \tag{3.4}$$

and hence we get

$$\Phi(X,Y) = \overline{\Phi}(X,Y)\Phi^*(X,Y), \tag{3.5}$$

and, by linearity in X, we see that

$$\begin{cases} \overline{F}(X,Y) \text{ and } \overline{\Phi}(X,Y) \text{ are irreducible in } \overline{k}_p(X)[Y], \\ \text{and so is } D_{q-1}(Y,a) - X \text{ for any } a \in \mathrm{GF}(q)^*. \end{cases} \tag{3.6}$$

Now clearly

$$\overline{\Phi}(X,Y) = Y^{q-1}(Y^{q-1} + Y^{1-q} - X)$$

and

$$D_{q-1}(Y,a) \neq Y^{q-1} + Y^{1-q} \quad \text{for all } a \in \mathrm{GF}(q)^*,$$

and hence

$$\overline{\Phi}(D_{q-1}(Y,a),Y) \neq 0 \quad \text{for all } a \in \mathrm{GF}(q)^*. \tag{3.7}$$

By (1.4) we also see that

$$D_{q-1}(Y,a) \neq D_{q-1}(Y,b) \quad \text{for all } a \neq b \text{ in } \mathrm{GF}(q)^*, \tag{3.8}$$

and therefore, working with polynomials in X over $k_q[Y]$, by (3.1) and (3.5) we conclude that

$$\Phi^*(X,Y) = \prod_{a \in \mathrm{GF}(q)^*} [D_{q-1}(Y,a) - X]. \tag{3.9}$$

By (2.5.3) we see that

$$\Phi^{(j)}(D_{q-1}(0,a),0) \neq 0 \quad \text{if } p > 2 \geq j \geq 1 \text{ and } a \in \mathrm{GF}(q)^* \setminus \mathrm{GF(q)}^{(j)}, \tag{3.10}$$

and hence

$$\Phi^{(j)}(D_{q-1}(Y,a),Y) \neq 0 \quad \text{if } p > 2 \geq j \geq 1 \text{ and } a \in \mathrm{GF}(q)^* \setminus \mathrm{GF(q)}^{(j)}. \tag{3.11}$$

Therefore, again working with polynomials in X over $k_q[Y]$, by (3.3) and (3.9) we conclude that

$$\Phi^{(j)}(X,Y) = \prod_{a \in \mathrm{GF}(q)^{(j)}} [D_{q-1}(Y,a) - X] \quad \text{if } p > 2 \geq j \geq 1. \tag{3.12}$$

Upon letting ζ be a primitive $(q-1)$-th root of 1 in $\mathrm{GF}(q)$, by (1.9) we get

$$D_{q-1}(\zeta^r Y, a) = D_{q-1}(Y, a\zeta^{-2r}) \quad \text{for } 1 \leq r \leq q-1 \text{ and } a \in \mathrm{GF}(q)^*. \tag{3.13}$$

In view of (3.13), by (3.8) and (3.9) we see that

$$\begin{cases} \text{if } p = 2, \text{ then we have} \\ D_{q-1}(\zeta^r Y, 1) \neq D_{q-1}(\zeta^s Y, 1) \text{ for } 1 \leq r < s \leq q-1, \\ \text{and } \Phi^*(X,Y) = \prod_{1 \leq r \leq q-1} [D_{q-1}(\zeta^r Y, 1) - X]. \end{cases} \tag{3.14}$$

For a moment assume that $p = 2$; then upon letting $J' = \overline{k}_p(X,Y)$ and $J = \overline{k}_p(X, Y^{q-1})$ we see that J' is a Galois extension of J and, for $1 \leq r \leq q-1$, the $q-1$ members of $\mathrm{Gal}(J', J)$ are given by $Y \mapsto \zeta^r Y$; therefore by (3.14) it follows that $\Phi^*(X,Y) = N_{J'/J}(D_{q-1}(Y,1) - X)$ and $F^*(X,Y)$ is irreducible in $\overline{k}_p(X)[Y]$;

for any field k between k_q and $\overline{k}_p$, upon letting $I' = k(X,Y)$ and $I = k(X,Y^{q-1})$, we clearly have $N_{I'/I}(D_{q-1}(Y,1) - X) = N_{J'/J}(D_{q-1}(Y,1) - X)$. Thus

$$\begin{cases} \text{if } p = 2, \text{ then } F^*(X,Y) \text{ is irreducible in } \overline{k}_p(X)[Y], \\ \text{and for any field } k \text{ between } k_q \text{ and } \overline{k}_p \text{ we have} \\ \Phi^*(X,Y) = N_{k(X,Y)/k(X,Y^{q-1})}(D_{q-1}(Y,1) - X). \end{cases} \tag{3.15}$$

In view of (3.13), by (3.8) and (3.12) we see that

$$\begin{cases} \text{if } p > 2, \text{ then, given any } l_j \in \mathrm{GF(q)}^{(j)} \text{ and } 1 \le j \le 2, \text{ we have} \\ D_{q-1}(\zeta^r Y, l_j) \ne D_{q-1}(\zeta^s Y, l_j) \text{ for } 1 \le r < s \le (q-1)/2, \\ \text{and } \Phi^{(j)}(X,Y) = \prod_{1 \le r \le (q-1)/2}[D_{q-1}(\zeta^r Y, l_j) - X]. \end{cases} \tag{3.16}$$

For a moment assume that $p > 2$ and let $l_j \in \mathrm{GF}(q)^{(j)}$ and $1 \le j \le 2$; then upon letting $J^* = \overline{k}_p(X, Y^2)$ and $J = \overline{k}_p(X, Y^{q-1})$ we see that J^* is a Galois extension of J and, for $1 \le r \le (q-1)/2$, the $(q-1)/2$ members of $\mathrm{Gal}(J^*, J)$ are given by $Y^2 \mapsto \zeta^{2r} Y^2$; therefore by (3.16) it follows that $\Phi^{(j)}(X,Y) = N_{J^*/J}(D_{q-1}(Y,l_j) - X)$ and $F^{(j)}(X,Y)$ is irreducible in $\overline{k}_p(X)[Y]$. For any field k between k_q and $\overline{k}_p$, letting $I^* = k(X,Y^2)$ and $I = k(X,Y^{q-1})$, we clearly have $N_{I^*/I}(D_{q-1}(Y,l_j) - X) = N_{J^*/J}(D_{q-1}(Y,l_j) - X)$. Thus

$$\begin{cases} \text{if } p > 2 \text{ and } 1 \le j \le 2, \text{ then } F^{(j)}(X,Y) \text{ is irreducible in } \overline{k}_p(X)[Y], \\ \text{and for any } l_j \in \mathrm{GF}(q)^{(j)} \text{ and any field } k \text{ between } k_q \text{ and } \overline{k}_p \text{ we have} \\ \Phi^{(j)}(X,Y) = N_{k(X,Y^2)/k(X,Y^{q-1})}(D_{q-1}(Y,l_j) - X). \end{cases} \tag{3.17}$$

This completes the proof of Theorems (1.T1)–(1.T3).

4. Galois Theory of Dickson Polynomials

To prove Theorem (1.T4), let n be a positive integer, let S_n, Z_n, DL_{2n} and MDL_n be as introduced in Section 1 before the statement of (1.T4), and let k be any field whose characteristic does not divide n and which contains a primitive n-th root ζ of 1.

For $0 \ne a \in k$, let $\overline{F}_a$ be the monic polynomial of degree 2 in Y over $k[X]$ given by

$$\overline{F}_a(X,Y) = Y^2 - XY + a^n, \tag{4.1}$$

and let $\overline{\Phi}_a$ be the monic polynomial of degree $2n$ in Y over $k[X]$ given by

$$\overline{\Phi}_a(X,Y) = \overline{F}_a(X,Y^n) = Y^{2n} - XY^n + a^n. \tag{4.2}$$

Let U_a be a root of $\overline{F}_a$, i.e., let U_a be an element in an algebraic closure Ω of $k(X)$ with $\overline{F}_a(X,U_a) = 0$. Then clearly

$$X = U_a + a^n U_a^{-1} \tag{4.3}$$

and

$$\overline{F}_a(X,Y) = (Y - U_a)(Y - a^n U_a^{-1}) \tag{4.4}$$

and

$$\mathrm{SF}(\overline{F}_a, k(X)) = k(U_a) \quad \text{and} \quad \mathrm{Gal}(k(U_a), k(X)) = Z_2, \tag{4.5}$$

where SF denotes the splitting field in Ω. Also, clearly,

$$\mathrm{Gal}(\overline{F}_a, k(X)) = S_2. \tag{4.6}$$

We can take $T_a \in \Omega$ with

$$T_a^n = U_a, \tag{4.7}$$

and then we get

$$\overline{\Phi}_a(X,Y) = \prod_{1\le i\le n} \left[(Y-\zeta^i T_a)(Y-\zeta^i a T_a^{-1})\right]. \tag{4.8}$$

Let $\mathrm{Aut}(k(T_a),k)$ be the group of all k-automorphisms of $k(T_a)$. Let $\sigma_a \in \mathrm{Aut}(k(T_a),k)$ be given by $T_a \mapsto \zeta T_a$, and let $\sigma_a' \in \mathrm{Aut}(k(T_a),k)$ be given by $T_a \mapsto aT_a^{-1}$. As usual let $\langle \sigma_a, \sigma_a'\rangle$ be the subgroup of $\mathrm{Aut}(k(T_a),k)$ generated by σ_a and σ_a'. Now clearly

$$\mathrm{SF}(\overline{\Phi}_a, k(X)) = k(T_a) \quad \text{and} \quad \mathrm{Gal}(k(T_a),k(X)) = \langle \sigma_a, \sigma_a'\rangle \approx DL_{2n}, \tag{4.9}$$

and

$$\mathrm{Gal}(\overline{\Phi}_a, k(X)) = DL_{2n}. \tag{4.10}$$

Moreover, $D_n(Y,a) - X$ is a monic irreducible polynomial of degree n in Y over $k[X]$, and by (1.6) we have

$$D_n(Y,a) - X = \prod_{1\le i\le n} (Y - \zeta^i T_a - \zeta^{-i} a T_a^{-1}), \tag{4.11}$$

and hence

$$\mathrm{SF}(D_n(Y,a)-X, k(X)) = \begin{cases} k(T_a) & \text{if } n \ge 3, \\ k(T_a + aT_a^{-1}) & \text{if } 1 \le n \le 2, \end{cases} \tag{4.12}$$

and therefore

$$\mathrm{Gal}(\mathrm{SF}(D_n(Y,a)-X, k(X)), k(X)) \approx MDL_n \tag{4.13}$$

and

$$\mathrm{Gal}(D_n(Y,a)-X, k(X)) = MDL_n. \tag{4.14}$$

Let Φ_1^* be the monic polynomial of degree n^2 in Y over $k[X]$ given by

$$\Phi_1^*(X,Y) = \prod_{1\le\lambda\le n} \left[D_n(Y,\zeta^\lambda) - X\right], \tag{4.15}$$

and let Φ_1 and $\widehat{\Phi}_1$ be the monic polynomials of degree $n(n+2)$ and $(n+1)^2$ in Y over $k[X]$ given by

$$\Phi_1(X,Y) = \overline{\Phi}_1(X,Y)\Phi_1^*(X,Y) \quad \text{and} \quad \widehat{\Phi}_1(X,Y) = Y\Phi_1(X,Y) \tag{4.16}$$

respectively. Let V^* be the set of cardinality n^2 given by

$$V^* = \{\zeta^r T_1 + \zeta^s T_1^{-1} : 1 \le r \le n \text{ and } 1 \le s \le n\}, \tag{4.17}$$

and let V and $\widehat{V}$ be the sets of cardinality $n(n+2)$ and $(n+1)^2$ given by

$$V = V^* \cup \{\zeta^i T_1 : 1 \le i \le n\} \cup \{\zeta^i T_1^{-1} : 1 \le i \le n\} \quad \text{and} \quad \widehat{V} = V \cup \{0\} \tag{4.18}$$

respectively. We can arrange matters so that

$$U_{\zeta^\lambda} = U_1 \quad \text{and} \quad T_{\zeta^\lambda} = T_1 \quad \text{for } 1 \le \lambda \le n,$$

and then by (4.11) we get

$$\Phi_1^*(X,Y) = \prod_{y\in V^*}(Y-y) \tag{4.19}$$

and

$$\mathrm{SF}(\Phi_1^*, k(X)) = \begin{cases} k(T_1) & \text{if } n \geq 2, \\ k(X) & \text{if } n = 1. \end{cases} \tag{4.20}$$

Therefore by (4.8) we get

$$\Phi_1(X,Y) = \prod_{y\in V}(Y-y) \quad \text{and} \quad \widehat{\Phi}_1(X,Y) = \prod_{y\in \widehat{V}}(Y-y) \tag{4.21}$$

and

$$\mathrm{SF}(\Phi_1, k(X)) = \mathrm{SF}(\widehat{\Phi}_1, k(X)) = k(T_1). \tag{4.22}$$

Let $S(V^*) = S_{n^2}$ be the symmetric group on V^*, and let $\tau^* \in S(V^*)$ and $\tau'^* \in S(V^*)$ be induced by σ_1 and σ_1' respectively. Again, as usual, let $\langle \tau^*, \tau'^* \rangle$ denote the subgroup of $S(V^*)$ generated by τ^* and τ'^*. Then, in view of (4.9), by (4.19) and (4.20) we see that

$$\mathrm{Gal}(\mathrm{SF}(\Phi_1^*, k(X)), k(X)) = \begin{cases} \langle \sigma_1, \sigma_1' \rangle \approx \langle \tau^*, \tau'^* \rangle \approx DL_{2n} & \text{if } n \geq 2, \\ Z_1 & \text{if } n = 1, \end{cases} \tag{4.23}$$

and

$$\mathrm{Gal}(\Phi_1^*, k(X)) = \begin{cases} \langle \tau^*, \tau'^* \rangle & \text{if } n \geq 2, \\ S_1 & \text{if } n = 1. \end{cases} \tag{4.24}$$

Let $S(V) = S_{n(n+2)}$ and $S(\widehat{V}) = S_{(n+1)^2}$ be the symmetric groups on V and $\widehat{V}$ respectively, let $\tau \in S(V)$ and $\tau' \in S(V)$ be induced by σ_1 and σ_1' respectively, and let $\widehat{\tau} \in S(\widehat{V})$ and $\widehat{\tau}' \in S(\widehat{V})$ be induced by σ_1 and σ_1' respectively. Again, as usual, let $\langle \tau, \tau' \rangle$ denote the subgroup of $S(V)$ generated by τ and τ', and let $\langle \widehat{\tau}, \widehat{\tau}' \rangle$ denote the subgroup of $S(\widehat{V})$ generated by $\widehat{\tau}$ and $\widehat{\tau}'$. Then, in view of (4.9), by (4.21) and (4.22) we see that

$$\mathrm{Gal}(k(T_1), k(X)) = \langle \sigma_1, \sigma_1' \rangle \approx \langle \tau, \tau' \rangle \approx \langle \widehat{\tau}, \widehat{\tau}' \rangle \approx DL_{2n} \tag{4.25}$$

and

$$\mathrm{Gal}(\Phi_1, k(X)) = \langle \tau, \tau' \rangle \quad \text{and} \quad \mathrm{Gal}(\widehat{\Phi}_1, k(X)) = \langle \widehat{\tau}, \widehat{\tau}' \rangle. \tag{4.26}$$

For $1 \leq i \leq n$ we have

$$\begin{aligned} \Phi_1^*(X, \zeta^i Y) &= \prod_{1\leq\lambda\leq n} \left[D_n(\zeta^i Y, \zeta^\lambda) - X \right] \quad \text{by (4.15)}, \\ &= \prod_{1\leq\lambda\leq n} \left[D_n(Y, \zeta^{\lambda-2i}) - X \right] \quad \text{by (1.9)} \\ &= \prod_{1\leq\lambda\leq n} \left[D_n(Y, \zeta^\lambda) - X \right] \quad \text{obviously} \\ &= \Phi_1^*(X,Y) \quad \text{by (4.15)}, \end{aligned}$$

and hence there exists a unique monic polynomial $F_1^*(X,Y)$ of degree n in Y over $k[X]$ such that

$$\Phi_1^*(X,Y) = F_1^*(X,Y^n). \tag{4.27}$$

In view of (4.17), by (4.19) and (4.27) we see that

$$F_1^*(X,Y) = \prod_{1\le i\le n} \left[Y - (\zeta^i T_1 + T_1^{-1})^n\right]. \tag{4.28}$$

Clearly

$$\begin{cases} \text{for } 1 \le i \le n \\ \text{we have } \sigma_1((\zeta^i T_1 + T_1^{-1})^n) = (\zeta^{i+2} T_1 + T_1^{-1})^n \\ \text{and } \sigma_1'((\zeta^i T_1 + T_1^{-1})^n) = (\zeta^{-i} T_1 + T_1^{-1})^n. \end{cases} \tag{4.29}$$

Let $\overline{k}$ be the algebraic closure of k in Ω.

By (4.28) we get

$$F_1^*(X,Y) = \prod_{1\le i\le n} \left[Y - (\zeta^{2i} T_1 + T_1^{-1})^n\right] \quad \text{for } n \text{ odd},$$

and therefore by (4.20), (4.23), (4.27) and (4.29) we see that

$$\text{if } n \text{ is odd, then } F_1^*(X,Y) \text{ is irreducible in } \overline{k}(X)[Y] \tag{4.30}$$

and

$$\mathrm{SF}(F_1^*, k(X)) = \begin{cases} k(T_1) & \text{for odd } n \ge 3, \\ k(X) & \text{for } n = 1, \end{cases} \tag{4.31}$$

and

$$\text{if } n \text{ is odd then } \mathrm{Gal}(F_1^*, k(X)) = MDL_n. \tag{4.32}$$

Let

$$W^{(1)} = \begin{cases} \{2,4,\dots,n\} & \text{if } n \equiv 2 \pmod 4, \\ \{1,3,\dots,n-1\} & \text{if } n \equiv 0 \pmod 4, \end{cases} \tag{4.33}$$

and

$$W^{(2)} = \begin{cases} \{2,4,\dots,n\} & \text{if } n \equiv 0 \pmod 4, \\ \{1,3,\dots,n-1\} & \text{if } n \equiv 2 \pmod 4, \end{cases} \tag{4.34}$$

and let

$$\Phi_1^{(j)}(X,Y) = \prod_{\lambda \in W^{(j)}} \left[D_n(Y, \zeta^\lambda) - X\right] \quad \text{for even } n \text{ and } 1 \le j \le 2. \tag{4.35}$$

Using an argument similar to the above argument, by (1.9) and (4.35) we see that

$$\Phi_1^{(j)}(X, \zeta^i Y) = \Phi_1^{(j)}(X,Y) \quad \text{for even } n \text{ and } 1 \le j \le 2 \text{ and } 1 \le i \le n,$$

and hence there exists a unique monic polynomial $F_1^{(j)}(X,Y)$ of degree $n/2$ in Y over $k[X]$ such that

$$\Phi_1^{(j)}(X,Y) = F_1^{(j)}(X,Y^n) \quad \text{for even } n \text{ and } 1 \le j \le 2. \tag{4.36}$$

Now obviously

$$\begin{cases} \text{if } n \text{ is even} \\ \text{then } \Phi_1^*(X,Y) = \Phi_1^{(1)}(X,Y)\Phi_1^{(2)}(X,Y) \\ \text{and } F_1^*(X,Y) = F_1^{(1)}(X,Y)F_1^{(2)}(X,Y). \end{cases} \tag{4.37}$$

Again, arguing as above, by (4.11), (4.28) and (4.29) we see that

$$F_1^{(j)}(X,Y) = \prod_{\lambda \in W^{(j)}} \left[Y - (\zeta^\lambda T_1 + T_1^{-1})^n\right] \quad \text{for even } n \text{ and } 1 \le j \le 2,$$

and

(4.38) if n is even and $1 \le j \le 2$, then $F_1^{(j)}(X,Y)$ is irreducible in $\overline{k}(X)[Y]$,

and

(4.39)

$$\mathrm{SF}(F_1^*, k(X)) = \mathrm{SF}(F_1^{(j)}, k(X)) = \begin{cases} k(T_1^2) & \text{for even } n \ge 6 \text{ and } 1 \le j \le 2, \\ k(X) & \text{for } n = 2 \text{ and } 1 \le j \le 2, \end{cases}$$

and

(4.40)

$$\mathrm{SF}(F_1^*, k(X)) = k(T_1^2) \text{ and } \mathrm{SF}(F_1^{(j)}, k(X)) = k((-1)^j T_1^2 + T_1^{-2}) \qquad \text{for } n = 4,$$

and

(4.41) if n is even and $1 \le j \le 2$, then $\mathrm{Gal}(F_1^{(j)}, k(X)) = MDL_{n/2}$.

Now Theorem (1.T4) follows from (4.6), (4.10), (4.14), (4.32), (4.39), (4.40) and (4.41) by taking $n = q-1$ and k to be any field between k_q and $\overline{k}_p$, and suppressing the subscripts a and 1.

Remark 4.42. Yet another incarnation of the dihedral group can be introduced by defining the twisted dihedral group TDL_{n+2} as the subgroup of S_{n+2} generated by the "rotation" $\widetilde{\sigma}$ given by $\widetilde{\sigma}(i) = i+1$ or 1 or i according as $1 \le i < n$ or $i = n$ or $n+1 \le i \le n+2$, and the "reflection" $\widetilde{\sigma}'$ given by $\widetilde{\sigma}'(n) = n$ together with $\widetilde{\sigma}'(i') = n - i'$ for $1 \le i' \le n-1$ as well as $\widetilde{\sigma}'(n+1) = n+2$ and $\widetilde{\sigma}'(n+2) = n+1$. Note that then we always have

$$TDL_{n+2} \approx DL_{2n}.$$

Moreover, if $n = q-1$ and $k = \mathrm{GF}(q)$, then, by taking $(1, 2, \ldots, n, n+1, n+2) = (\zeta, \zeta^2, \ldots, \zeta^n, 0, \infty)$, the group TDL_{n+2} gets identified with the image of $\langle \sigma_1, \sigma_1' \rangle$ under the natural isomorphism $\mathrm{Aut}(k(T_1), k) \to \mathrm{PGL}(2, q)$.

5. Orthogonal Groups and Dickson Polynomials

In the situation of Section 4, let $n = q-1$ and let k be any field between k_q and $\overline{k}_p$. Then $\widehat{V} = \{vT_1 + wT_1^{-1} : (v,w) \in \mathrm{GF}(q)^2\}$ is a 2 dimensional vector space over $\mathrm{GF}(q)$, and $\langle \widehat{\tau}, \widehat{\tau}' \rangle$ is the isometry group for the quadratic form $vT_1 + wT_1^{-1} \mapsto vw$. Therefore by (4.26) we have $\mathrm{Gal}(\widehat{\Phi}, k(X)) = \mathrm{O}^+(2,q)$, and therefore (see Proposition 3.1 on page 16 of [Ab3]) we get $\mathrm{Gal}(F, k(X)) = \mathrm{PO}^+(2,q)$.

This completes the proof of Theorem (1.T5).

References

[Ab1] S. S. Abhyankar, *Coverings of algebraic curves*, American Journal of Mathematics **79** (1957), 825-856. MR **20:**872

[Ab2] S. S. Abhyankar, *Galois theory on the line in nonzero characteristic*, Bulletin of the American Mathematical Society **27** (1992), 68-133. MR **94a:**12004

[Ab3] S. S. Abhyankar, *Nice equations for nice groups*, Israel Journal of Mathematics **88** (1994), 1-24. MR **96f:**12003

[Ab4] S. S. Abhyankar, *Fundamental group of the affine line in positive characteristic*, Proceedings of the 1992 International Colloquium on Geometry and Analysis, Tata Institute of Fundamental Research, Bombay (1995), 1-26. MR **97b:**14034

[Ab5] S. S. Abhyankar, *Again nice equations for nice groups*, Proceedings of the American Mathematical Society **124** (1996), 2967-2976. MR **96m:**12004

[Ab6] S. S. Abhyankar, *More nice equations for nice groups*, Proceedings of the American Mathematical Society **124** (1996), 2977-2991. MR **96m:**12005

[Ab7] S. S. Abhyankar, *Further nice equations for nice groups*, Transactions of the American Mathematical Society **348** (1996), 1551-1577. MR **96m:**14021

[Ab8] S. S. Abhyankar, *Factorizations over finite fields*, Finite Fields and Applications, London Mathematical Society, Lecture Note Series **233** (1996), 1-21. MR **98c:**11130

[CM1] S. D. Cohen and R. Matthews, *Exceptional polynomials over finite fields*, Finite Fields and Their Applications **1** (1995), 261-277. MR **96e:**11158

[CM2] S. D. Cohen and R. Matthews, *Monodromy groups of classical families over finite fields*, Finite Fields and Applications, London Mathematical Society, Lecture Note Series **233** (1996), 59-68. MR **98f:**11131

[Di1] L. E. Dickson, *The analytic presentation of substitutions on a power of a prime number of letters with a discussion of the linear group*, Annals of Mathematics **11** (1897), 65-120.

[Di2] L. E. Dickson, *Linear Groups*, Teubner, 1901.

[KLi] P. Kleidman and M. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, Cambridge University Press, 1990. MR **91g:**20001

[Lie] M. Liebeck, *Characterization of classical groups by orbit sizes on the natural module*, Proceedings of the American Mathematical Society **124** (1996), 2961-2966. MR **97e:**20068

[LMT] R. Lidl, G.L. Mullen, and G. Turnwald, *Dickson Polynomials*, Longman, 1993. MR **94i:**11097

[Sch] I. Schur, *Über den Zusammenhang zwischen einemem Problem der Zahlentheorie und einem Satz über algebraische Funktionen*, Sitzungsber. Akad. Wiss. Berlin (1923), 123-134.

Department of Mathematics, Purdue University, West Lafayette, Indiana 47907
E-mail address: ram@cs.purdue.edu

Department of Mathematics, University of Glasgow, Glasgow G12 8QW, Scotland
E-mail address: sdc@maths.gla.ac.uk

Department of Mathematics, University of Southern California, Los Angeles, California 90089
E-mail address: zieve@math.brown.edu