PACIFIC JOURNAL OF MATHEMATICS
Vol. 34, No. 2, 1970

FINITE TRANSFORMATION FORMULAE INVOLVING THE LEGENDRE SYMBOL

KENNETH S. WILLIAMS

Let p denote an odd prime. The following three identities (transformation formulae) involving the Legendre symbol $\left(\frac{\ }{p}\right)$ are known to be valid for any complex-valued function F defined on the integers, which is periodic with period p:

$$\sum_{x=0}^{p-1} F(x) + \sum_{x=0}^{p-1}\left(\frac{x}{p}\right)F(x) = \sum_{x=0}^{p-1} F(x^2) ,$$

$$\sum_{x=0}^{p-1} F(x) + \sum_{x=0}^{p-1}\left(\frac{x^2-4a}{p}\right)F(x) = \sum_{x=1}^{p-1} F\left(x+\frac{a}{x}\right) , \quad a \not\equiv 0 \pmod p ,$$

$$\sum_{x=0}^{p-1} F(x) + \sum_{x=0}^{p-1}\left(\frac{x^2-4x}{p}\right)F(x) = \sum_{x=1}^{p-1} F\left(x+2+\frac{1}{x}\right) .$$

We consider a general class of transformation formulae, which includes the above examples.

Let p denote a fixed odd prime and let GF(p) denote the Galois field with p elements. If X denotes an indeterminate we let

$$\Theta[X] = \left\{\theta(X) = \frac{aX^2+bX+c}{AX^2+BX+C} \,\middle|\, a, b, c, A, B, C \in \mathrm{GF}(p), \right.$$
$$\left. (aC-cA)^2 - (aB-bA)(bC-cB) \neq 0\right\}$$

and

$$\Phi[X] = \{\phi(X) = qX^2 + rX + s \mid q, r, s \in \mathrm{GF}(p), r^2 - 4qs \neq 0\} .$$

Corresponding to any element $\theta(X) \in \Theta[X]$ (often just written $\theta \in \Theta$) we define

$$\theta^*(X) = DX^2 + \Delta X + d ,$$

where

$$D = B^2 - 4AC, \Delta = 4aC - 2bB + 4cA, d = b^2 - 4ac .$$

It is clear that $\theta^*(X) \in \Phi[X]$ as

$$\Delta^2 - 4Dd = 16\{(aC-cA)^2 - (aB-bA)(bC-cB)\} \neq 0 .$$

For any element $\phi(X) \in \Phi[X]$ (often just written $\phi \in \Phi$) its value at $x \in \mathrm{GF}(p)$ is just $\phi(x) = qx^2 + rx + s \in \mathrm{GF}(p)$. For any element $\theta(X) \in \Theta[X]$, $\theta(x)$ will be defined provided $Ax^2 + Bx + C \neq 0$ and its value is

$$\theta(x) = \frac{ax^2+bx+c}{Ax^2+Bx+C} = (ax^2+bx+c)(Ax^2+Bx+C)^{-1} \in \mathrm{GF}(p) .$$

Throughout this paper whenever we write $\sum_x$ the summation is taken over all $x \in \mathrm{GF}(p)$. If we write $\sum_x'$ the summation is over all $x \in \mathrm{GF}(p)$ for which the summand is defined.

Further we let $\mathscr{C}$ denote the complex number field and we denote by $\mathscr{F}$ the set of all functions with domain GF(p) and range $\subseteqq \mathscr{C}$. The particular function $\chi \in \mathscr{F}$ defined for any $x \in \mathrm{GF}(p)$ by

$$\chi(x) = \begin{cases} 0, \text{ if } x = 0, \\ 1, \text{ if } x \neq 0 \text{ and there exists } y \in \mathrm{GF}(p) \text{ such that } y^2 = x, \\ -1, \text{ if } x \neq 0 \text{ and no such } y \text{ exists,} \end{cases}$$

plays a special role in what we do. χ is the Legendre symbol on GF(p). Finally for $(F, \theta) \in \mathscr{F} \times \Theta$ we define

$$\delta(F, \theta) = \begin{cases} F(a/A), \text{ if } A \neq 0 , \\ 0 \qquad\quad , \text{ if } A = 0 . \end{cases}$$

We are now in a position to define what we mean by the transformation formula $T(\theta, \phi)$.

DEFINITION. If $(\theta, \phi) \in \Theta \times \Phi$ is such that

$$\sum_x F(x) + \sum_x \chi(\phi(x))F(x) = \sum_x{}' F(\theta(x)) + \delta(F, \theta) ,$$

for *all* $F \in \mathscr{F}$, we say that the *transformation formula* $T(\theta, \phi)$ is valid. If on the other hand there is some $F_0 \in \mathscr{F}$ such that

$$\sum_x F_0(x) + \sum_x \chi(\phi(x))F_0(x) \neq \sum_x{}' F_0(\theta(x) + \delta(F_0, \theta)) ,$$

then we say that $T(\theta, \phi)$ is *not* valid.

In some special cases it is well-known that $T(\theta, \phi)$ is valid. For example ([1; p. 159], [4; p. 101]) it is known that $T(\theta, \phi)$ is valid if

$$\theta(X) = X^2, \phi(X) = X \tag{1.1}$$

or

$$\theta(X) = \frac{X^2 + c}{X}, \phi(X) = X^2 - 4c \qquad (c \neq 0) . \tag{1.2}$$

(We identify the elements of GF(p) with the residues modulo p and the elements of $\mathscr{F}$ with functions defined on the integers which are periodic with period p). The name *transformation formula* is justified as (1.1) (resp. (1.2)) gives the well-known transformation property of the Gauss (resp. Kloosterman) sum, if we take $F(x) = \exp(2\pi ix/p)$, [3], [4]. Both examples mentioned above have $\delta(F, \theta) = 0$. An example with $\delta(F, \theta) \neq 0$ in general, is given by the following

$$(1.3) \qquad \sum_x F(x) + \sum_x \chi(4x+1)F(x) = \sum_x{}' F\left(\frac{x+1}{x^2}\right) + F(0) .$$

Here

$$\theta(X) = \frac{X+1}{X^2} \text{ and } \phi(X) = 4X + 1 .$$

The main objective of this paper is to give necessary and sufficient conditions for $T(\theta, \phi)$ to be valid. We prove in § 4 that if $(\theta, \phi) \in \Theta \times \Phi$ then $T(\theta, \phi)$ is valid if and only if there exists $e(\neq 0) \in \mathrm{GF}(p)$ such that $\phi = e^2\theta^*$. (We note that in (1.1) $\theta^*(X) = 4X = 4\phi(X)$, in (1.2) $\theta^*(X) = X^2 - 4c = \phi(X)$ and in (1.3) $\theta^*(X) = 4X + 1 = \phi(X)$). The proof of these necessary and sufficient conditions requires a useful lemma concerning quadratic polynomials possessing the same quadratic nature. This lemma is proved in § 3. In § 2 a number of properties of $\Theta[X]$ and $\Phi[X]$ are noted, which together with the main theorem enable us to deduce that there are only two essentially different transformation formulae $T(\theta, \phi)$.

2. Properties of $\Theta[X]$ and $\Phi[X]$. We first consider $\Theta[X]$. The elements $\theta(X) = aX^2 + bX + c/AX^2 + BX + C$ of $\Theta[X]$ are well-defined, as A, B, C cannot all be zero. Further they do not reduce to the form $lX + m/LX + M$, as not both of a, A are zero and $aX^2 + bX + c$ and $AX^2 + BX + C$ do not have a nonunit common factor.

Any element of $\Theta[X]$ gives rise to another element of $\Theta[X]$ in the following way. If $t, u, v, w, k, l, m, n \in \mathrm{GF}(p)$ are such that

$$tw - uv \neq 0, kn - lm \neq 0 ,$$

and if $\theta(X) \in \Theta[X]$ then so does

$$(2.1) \qquad \theta_1(X) = \frac{t\theta\left(\dfrac{kX+l}{mX+n}\right) + u}{v\theta\left(\dfrac{kX+l}{mX+n}\right) + w} .$$

The proof of this just consists of showing that

$$\theta_1(X) = \frac{a_1X^2 + b_1X + c_1}{A_1X^2 + B_1X + C_1} ,$$

where

$$\begin{aligned} a_1 &= (ta + uA)k^2 + (tb + uB)km + (tc + uC)m^2 , \\ b_1 &= 2(ta + uA)kl + (tb + uB)(kn + lm) + 2(tc + uC)mn , \\ c_1 &= (ta + uA)l^2 + (tb + uB)ln + (bc + uC)n^2 , \\ A_1 &= (va + wA)k^2 + (vb + wB)km + (vc + wC)m^2 , \end{aligned}$$

$$B_1 = 2(va + wA)kl + (vb + wB)(kn + lm) + 2(vc + wC)mn\ ,$$
$$C_1 = (va + wA)l^2 + (vb + wB)ln + (vc + wC)n^2\ ,$$

and noting that

$$\begin{aligned}&(a_1C_1 - c_1A_1)^2 - (a_1B_1 - b_1A_1)(b_1C_1 - c_1B_1)\\ (2.2)\qquad &= (tw - uv)^2(kn - lm)^4\{(aC - cA)^2 - (aB - bA)(bC - cB)\}\\ &\neq 0\ .\end{aligned}$$

We can thus define on equivalence relation on $\Theta[X]$ by saying that $\theta(X), \theta_1(X) \in \Theta[X]$ are equivalent if there exist $k, l, m, n, t, u, v, w \in \mathrm{GF}(p)$ with $kn - lm \neq 0$, $tw - uv \neq 0$ and such that (2.1) holds. We write $\theta_1 \sim \theta$.

Let c_1 and c_2 be fixed elements of GF(p) such that $\chi(c_1) = +1$, $\chi(c_2) = -1$, so that there exists $d_1(\neq 0) \in \mathrm{GF}(p)$ with $c_1 = d_1^2$. Then any element

$$\theta(X) = \frac{aX^2 + bX + c}{AX^2 + BX + C} \in \Theta[X]$$

is either equivalent to $\theta_{c_1}(X) = X + (c_1/X)$ or $\theta_{c_2}(X) = X + (c_2/X)$. More precisely we have

$$\theta \sim \theta_{c_1},\ \text{if}\ \chi((aC - cA)^2 - (aB - bA)(bC - cB)) = +1$$

and

$$\theta \sim \theta_{c_2},\ \text{if}\ \chi((aC - cA)^2 - (aB - bA)(bC - cB)) = -1\ .$$

This is clear as we have

$$\theta(X) = \frac{t\theta_{c_1}\left(\dfrac{kX + l}{mX + n}\right) + u}{v\theta_{c_1}\left(\dfrac{kX + l}{mX + n}\right) + w}\ ,$$

where

(i) $t = ah$, $u = b - 2ag$, $v = Ah$, $w = B - 2Ag$, $k = 1$, $l = g$, $m = 0$, $n = h$, if $\chi((aC - cA)^2 - (aB - bA)(bC - cB)) = +1$, $aB - bA \neq 0$, and g and $h(\neq 0) \in \mathrm{GF}(p)$ are defined by

$$g = \frac{aC - cA}{aB - bA},\ c_1h^2 = \left(\frac{aC - cA}{aB - bA}\right)^2 - \left(\frac{bC - cB}{aB - bA}\right);$$

(ii) $t = aA(1 - d)$, $u = 2aAd_1(1 + d)$, $v = A^2 - a^2D$, $w = 2d_1(A^2 + a^2D)$, $k = 2ad_1$, $l = (b + 1)d_1$, $m = 2a$, $n = (b - 1)$, if $\chi((aC - cA)^2 - (aB - bA)(bC - cB)) = +1$, $aB - bA = 0$, $aA \neq 0$;

(iii) $t = a^2C^2 - d$, $u = 2d_1(a^2C^2 + d)$, $v = 4aC$, $w = -8d_1aC$, $k = 2ad_1$, $l = d_1(b + aC)$, $m = 2a$, $n = b - aC$, if $\chi((aC - cA)^2 - (aB - bA)(bC - cB)) = +1$, $aB - bA = 0$, $A = 0$;

(iv) $t = 4Ac$, $u = -8d_1Ac$, $v = A^2c^2 - D$, $w = 2d_1(A^2c^2 + D)$, $k = 2d_1A$, $l = d_1(B + Ac)$, $m = 2A$, $n = B - Ac$, if $\chi((aC - cA)^2 - (aB - bA)(bC - cB)) = +1$, $aB - bA = 0$, $a = 0$;
and

$$\theta(X) = \frac{t\theta_{c_2}\left(\dfrac{kX + l}{mX + n}\right) + u}{v\theta_{c_2}\left(\dfrac{kX + l}{mX + n}\right) + w},$$

where

(v) $t = ah, u = b - 2ag, v = Ah, w = B - 2Ag, k = 1, l = g, m = 0, n = h$, if $\chi((aC - cA)^2 - (aB - bA)(bC - cB)) = -1$ and g, h are defined by

$$g = \frac{aC - cA}{aB - bA}, c_2h^2 = \left(\frac{aC - cA}{aB - bA}\right)^2 - \left(\frac{bC - cB}{aB - bA}\right).$$

This shows that there are atmost two equivalence classes in $\Theta[X]$. We show that there are exactly two by proving that $\theta_{c_1}(X) \not\sim \theta_{c_2}(X)$. For suppose that $\theta_{c_1}(x) \sim \theta_{c_2}(x)$ then there exist $k, l, m, n, t, u, v, w \in \mathrm{GF}(p)$ with

$$kn - lm \neq 0, tw - uv \neq 0$$

and such that

$$\theta_{c_1}(X) = \frac{t\theta_{c_2}\left(\dfrac{kX + l}{mX + n}\right) + u}{t\theta_{c_2}\left(\dfrac{kX + l}{mX + n}\right) + w}.$$

Thus from (2.2) we have

$$-c_1 = (tw - uv)^2(kn - lm)^3(-c_2),$$

which contradicts that $\chi(c_1) = +1, \chi(c_2) = -1$.

We now consider $\Phi[X]$. The elements $\phi(X) = qX^2 + rX + s$ of $\Phi[X]$ are either genuinely quadratic or linear, as q, r are not both zero. Moreover they are not of the form $q(X + k)^2$, for any $k \in \mathrm{GF}(p)$. Corresponding to (2.1) we have

$$\theta_1^*(X) = (kn - lm)^2(-vX + t)^2\theta^*\left(\frac{wX - u}{vX + t}\right) \in \Phi[X].$$

3. A useful lemma. We prove the following lemma which is needed in the proof of our theorem.

LEMMA. *If* $qX^2 + rX + s, q'X^2 + r'X + s' \in \Phi[X]$ *are such that* $\chi(qx^2 + rx + s) = \chi(q'x^2 + r'x + s')$, *for all* $x \in \mathrm{GF}(p)$, *then there exists*

$e(\neq 0) \in \mathrm{GF}(p)$ *such that*

$$qX^2 + rX + s = e^2(q'X^2 + r'X^2 + r'X + s') .$$

Proof. As $qX^2 + rX + s \in \Phi[X]$ it is not of the form $q(X+k)^2$ and not both of q, r are zero, similarly for $q'X^2 + r'X + s'$. The condition $\chi(qx^2 + rx + s) = \chi(q'x^2 + r'x + s')$ implies that a zero of $qx^2 + rx + s$ is a zero of $q'x^2 + r'x + s'$ and vice-versa. Thus, unless both $qX^2 + rX + s$ and $q'X^2 + r'X + s'$ are irreducible in $\mathrm{GF}(p)[X]$, that is, unless $\chi(r^2 - 4qs) = \chi(r'^2 - 4q's') = -1$, we have for some $e_1, e_2 \in \mathrm{GF}(p)(e_1 \neq e_2)$ either

$$qX^2 + rX + s = q(X - e_1)(X - e_2),\ q'X^2 + r'X + s' = q'(X - e_1)(X - e_2),\quad q, q' \neq 0 ,$$

or

$$qX^2 + rX + s = r(X - e_1),\ q'X^2 + r'X + s' = r'(X - e_1),\ q = q' = 0 .$$

In the former case taking $x \neq e_1, e_2$ in

$$\chi(qx^2 + rx + s) = \chi(q'x^2 + r'x + s')$$

we obtain $\chi(q) = \chi(q')$, so that there exists $e(\neq 0) \in \mathrm{GF}(p)$ such that $q = e^2 q'$. Hence

$$r = -q(e_1 + e_2) = -e^2 q'(e_1 + e_2) = e^2 r',\ s = qe_1e_2 = e^2 q' e_1 e_2 = e^2 s'$$

and so we have

$$qx^2 + rX + s = e^2(q'X^2 + r'X + s') .$$

In the latter case taking $x \neq e_1$ in $\chi(qx^2 + rx + s) = \chi(q'x^2 + r'x + s')$ we obtain $\chi(r) = \chi(r')$, so that there exists $e(\neq 0) \in \mathrm{GF}(p)$ such that $r = e^2 r'$. Hence $s = -re_1 = e^2 r' e_1 = e^2 s'$ and we have

$$qX^2 + rX + s = e^2(q'X^2 + r'X + s') .$$

If $\chi(r^2 - rqs) = \chi(r'^2 - rq's') = -1$ then $q, q', r^2 - 4qs, r'^2 - 4q's'$ are all nonzero and

$$\sum_x \chi(qx^2 + rx + s) = \sum_x \chi(q'x^2 + r'x + s')$$

gives $\chi(q) = \chi(q')$. Hence there exists $e(\neq 0) \in \mathrm{GF}(p)$ such that $q = e^2 q'$. Now as $qq' = (eq')^2 \neq 0$ we have

$$\sum_x \chi\Big(\Big(x^2 + \frac{r}{q}x + \frac{s}{q}\Big)\Big(x^2 + \frac{r'}{q'}x + \frac{s'}{q'}\Big)\Big)$$
$$= \sum_x \chi((qx^2 + rx + s)(q'x^2 + r'x + s'))$$

$$= \sum_x \chi((qx^2 + rx + s)^2)$$
$$= \sum_x 1$$

and so

$$\sum_x \chi\left(\left(x^2 + \frac{r}{q}x + \frac{s}{q}\right)\left(x^2 + \frac{r'}{q'}x + \frac{s'}{q'}\right)\right) = p\ . \tag{3.1}$$

If $X^2 + (r/q)X + (s/q) \neq X^2 + (r'/q')X + (s'/q')$ then by a deep result of Perel'muter [2] we have

$$\left|\sum_x X\left(\left(x^2 + \frac{r}{q}x + \frac{s}{q}\right)\left(x^2 + \frac{r'}{q'}x + \frac{s'}{q'}\right)\right)\right| \leqq 2p^{1/2}\ .$$

For $p \geqq 5$ this clearly contradicts (3.1). Thus for $p \geqq 5$ we have $X^2 + (r/q)X + (s/q) = X^2 + (r'/q')X + (s'/q')$, that is as $q = e^2q'$,

$$qX^2 + rX + s = e^2(q'X^2 + r'X + t')\ ,$$

as required. When $p = 3$ the theorem is easily verified by examining the values of $qx^2 + rx + s$ for $x \in \mathrm{GF}(p)$ (see table).

When $p = 3$, $\Phi[X]$ consists of all polynomials of GF(3)$[X]$ of degree atmost 2 except the 9 polynomials $q(X + k)^2$, $q, k \in \mathrm{GF}(3)$, which have discriminant equal to zero. The table shows that there do not exist 2 elements of $\Phi[X]$, say $\phi(X), \phi'(X)$ with $\chi(\phi(x)) = \chi(\phi'(x))$, for all $x \in \mathrm{GF}(3)$.

TABLE.

$\phi(X) \in \Phi[X]$	$\chi(\phi(0))$	$\chi(\phi(1))$	$\chi(\phi(2))$
X	0	1	−1
$X+1$	1	−1	0
$X+2$	−1	0	1
$2X$	0	−1	1
$2X+1$	1	0	−1
$2X+2$	−1	1	0
X^2+1	1	−1	−1
X^2+2	−1	0	0
X^2+X	0	−1	0
X^2+X+2	−1	1	−1
X^2+2X	0	0	−1
X^2+2X+2	−1	−1	1
$2X^2+1$	1	0	0
$2X^2+2$	−1	1	1
$2X^2+X$	0	0	1
$2X^2+X+1$	1	1	−1
$2X^2+2X$	0	1	0
$2X^2+2X+1$	1	−1	1

4. Main result. We prove

THEOREM. *If* $(\theta, \phi) \in \Theta \times \Phi$ *then* $T(\theta, \phi)$ *is valid if and only if there exists* $e(\neq 0) \in \mathrm{GF}(p)$ *such that*

$$\phi = e^2\theta^* . \tag{4.1}$$

Proof. (i) We let $\phi = e^2\theta^*$, where $e(\neq 0) \in \mathrm{GF}(p)$ and

$$\theta(X) = \frac{aX^2 + bX + c}{AX^2 + BX + C} \in \Theta[X] ,$$

and prove that $T(\theta, \phi)$ is valid. For all $F \in \mathscr{F}$ we have

$$\begin{aligned}\sum_x{}' F(\theta(x)) &= \sum_y \sum_{\substack{x \\ \theta(x)=y}}{}' F(\theta(x)) \\ &= \sum_y F(y) \sum_{\substack{x \\ \theta(x)=y}}{}' 1 .\end{aligned}$$

Thus for given $y \in \mathrm{GF}(p)$ we require the number of solutions $x \in \mathrm{GF}(p)$ of $\theta(x) = y$, that is of

$$(Ay - a)x^2 + (By - b)x + (Cy - c) = 0 . \tag{4.2}$$

This is a genuine quadratic in x unless $Ay - a = 0$. Thus we must consider two cases according as $A = 0$ or $A \neq 0$.

Case (*a*). $A = 0$, (so that $\delta(F, \theta) = 0$).
In this case $a \neq 0$ so that $Ay - a \neq 0$, for all $y \in \mathrm{GF}(p)$. Thus the number of solutions of (4.2) is

$$\begin{aligned}&1 + \chi((By - b)^2 - 4(Ay - a)(Cy - c)) \\ &= 1 + \chi(Dy^2 + \Delta y + d) \\ &= 1 + \chi(\phi(y)), \text{ as } e \neq 0 .\end{aligned}$$

Hence we have

$$\sum_x{}' F(\theta(x)) = \sum_y F(y) + \sum_y \chi(\phi(y))F(y) ,$$

proving that $T(\theta, \phi)$ is valid in the case.

Case (*b*). $A \neq 0$, (so that $\delta(F, \theta) = F(a/A)$).
In this case, for all $y \in \mathrm{GF}(p)$ except a/A, (4.2) is a genuine quadratic and the number of solutions of it, for such y, is as in case (a). For $y = a/A$, (4.2) becomes

$$(aB - bA)x + (aC - cA) = 0 ,$$

which since $aB - bA$ and $aC - cA$ cannot both be zero, has one solution if $aB - bA \neq 0$ and no solutions if $aB - bA = 0$. This number is expressible as $\chi((aB - bA)^2)$. Hence

$$\begin{aligned}&\sum_x{}' F(\theta(x)) + \delta(F, \theta)\\ &= F(a/A)\chi((aB - bA)^2) + \sum_{y \neq a/A} \{1 + \chi(Dy^2 + \Delta y + d)\} F(y) + F(a/A)\\ &= \sum_y \{1 + \chi(e^2\theta^*(y))\} F(y)\end{aligned}$$

as required, since

$$A^2\left(D\left(\frac{a}{A}\right)^2 + \Delta\left(\frac{a}{A}\right) + d\right) = (aB - bA)^2 .$$

(ii) Conversely we show that if $(\theta, \phi) \in \Theta \times \Phi$ is such that $T(\theta, \phi)$ is valid then $\phi(X) = e^2\theta^*(X)$. For *all* $F \in \mathscr{F}$, as $T(\theta, \phi)$ is valid, we have

$$\sum_x{}' F(\theta(x)) + \delta(F, \theta) = \sum_x F(x) + \sum_x \chi(\phi(x)) F(x) . \tag{4.3}$$

From (i) we know that $T(\theta, \theta^*)$ is valid, so that also for all $F \in \mathscr{F}$ we have

$$\sum_x{}' F(\theta(x)) + \delta(F, \theta) = \sum_x F(x) + \sum_x \chi(Dx^2 + \Delta x + d) F(x) . \tag{4.4}$$

Hence form (4.3) and (4.4) we have

$$\sum_x \chi(\phi(x)) F(x) = \sum_x \chi(Dx^2 + \Delta x + d) F(x) , \tag{4.5}$$

for all $F \in \mathscr{F}$. In particular taking $F = F_r (r \in \mathrm{GF}(p))$ in (4.5) where F_r is defined for $x \in \mathrm{GF}(p)$ by

$$F_r(x) = \begin{cases} 1, & x = r , \\ 0, & x \neq r , \end{cases}$$

we have

$$\chi(\phi(r)) = \chi(Dr^2 + \Delta r + d) ,$$

for all $r \in \mathrm{GF}(p)$. By lemma as $\phi(X), DX^2 + \Delta X + d \in \Phi[X]$, we have, for some $e(\neq 0) \in \mathrm{GF}(p)$,

$$\phi(X) = e^2(DX^2 + \Delta X + d) = e^2\theta^*(X) ,$$

which is (4.1).

5. An application. We use the theorem to evaluate the Salié sum [4]. Let $\theta(X) = (X + 1)^2/X$ so that $\theta^*(X) = X^2 - 4X$. By the theorem we know that $T(\theta, \theta^*)$ is valid. If $G \in \mathscr{F}$ so does χG. Taking $F(x) = \chi(x)G(x)$ in $T(\theta, \theta^*)$ we obtain

$$\sum_x \chi(x)G(x) + \sum_x \chi(x^2(x-4))G(x) = \sum_x{}' \chi\left(\frac{(x+1)^2}{x}\right)G\left(\frac{(x+1)^2}{x}\right)$$

that is,

$$\sum_x \chi(x)G(x) + \sum_x \chi(x-4)G(x) = \sum_x{}' \chi(x)G\left(x+2+\frac{1}{x}\right). \tag{5.1}$$

Taking $G(x) = \exp(2\pi ikx/p)$ and noting that this choice makes the two sums on the left hand side of (5.1) Gaussian sums we obtain Salié's result [4]

$$\sum_{x\neq 0} \chi(x) \exp\left(\frac{2\pi ik}{p}\left(x + \frac{1}{x}\right)\right) = 2\left(\frac{k}{p}\right)i^{1/4(p-1)^2}p^{1/2}\cos\left(\frac{4\pi k}{p}\right).$$

6. Conclusion. The properties of $\Theta[X]$ indicated in § 2 and the theorem of § 4 show that there are only two essentially different transformation formulae $T(\theta, \phi)$ given by $(\theta, \phi) = (\theta_{c_1}, \theta^*_{c_1})$ and $(\theta_{c_2}, \theta^*_{c_2})$, where we have identified $T(\theta, \theta^*)$ and $T(\theta, e^2\theta^*)$. It would be interesting to know if this work could be generalized to give results concerning identities of a type similar to $T(\theta, \phi)$ but where θ, ϕ are elements of larger sets than Θ, Φ respectively and/or where χ is replaced by a more general character.

I would like to finish by thanking an unknown referee for a number of valuable suggestions. In particular he suggested the proof of the lemma given in § 3, which considerably shortened my original proof.

References

1. H. Davenport, *On certain exponential sums*, J. für Math. **169** (1933), 158–176.
2. G. I. Perel'muter, *On certain sums of characters*, Uspehi Mat. Nauk. **18** (1963), 145–149.
3. H. Rademacher, *Lectures on elementary number theory*, Blaisdell, 1964.
4. H. Salié, *Über die Kloostermanschen Summen* $S(u, v; q)$, Math. Zeit. **34** (1931), 91–109.

Received August 26, 1969, and in revised form January 30, 1970. This research was supported by a National Research Council of Canada Grant (No. A-7233).

CARLETON UNIVERSITY
OTTAWA, CANADA