

## §2. L-FUNCTIONS

Objektyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **37 (1991)**

Heft 3-4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **20.09.2024**

### **Nutzungsbedingungen**

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

### **Haftungsausschluss**

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

*Acknowledgement.* We are very grateful to G. W. Anderson for helpful correspondence on  $L$ -functions and character sums.

## §2. $L$ -FUNCTIONS

Throughout this section,  $V$  denotes a *monic* polynomial over  $GF(q)$ , and  $v$  ranges over the distinct monic irreducible factors of  $V$  over  $GF(q)$ . Write

$$(2.1) \quad V = \prod_{v|V} v^{\text{ord}_v V}, \quad F = F_V = \prod_{v|V} v.$$

If no exponent  $\text{ord}_v V$  in (2.1) is divisible by  $q - 1$ , then  $V$  is said to be *primitive*. Note that  $V = 1$  is primitive. For any monic polynomial

$$(2.2) \quad W = W(x) = x^n + w_{n-1}x^{n-1} + w_{n-2}x^{n-2} + \cdots + w_0$$

over  $GF(q)$ , set

$$(2.3) \quad \alpha(W) = w_{n-1}, \quad \beta(W) = w_{n-1}^2/2 - w_{n-2}.$$

Define the  $L$ -functions

$$(2.4) \quad L(t, V) = \sum_W \tau(R(V, W)) t^{\deg W},$$

$$(2.4a) \quad L_1(t, V) = \sum_W \psi(\alpha(W)) \tau(R(V, W)) t^{\deg W},$$

$$(2.4b) \quad L_2(t, V) = \sum_W \psi(\beta(W)) \tau(R(V, W)) t^{\deg W},$$

where in each sum,  $W$  ranges over all monic polynomials over  $GF(q)$ , and  $R(V, W)$  is the resultant of  $V$  and  $W$ . It is easily checked that

$$(2.5) \quad \begin{aligned} L(t, 1) &= (1 - qt)^{-1}, & L_1(t, 1) &= 1, \\ L_2(t, 1) &= 1 + \phi(2)G((q-1)/2)t. \end{aligned}$$

Since the summands in (2.4), (2.4a), (2.4b) are multiplicative in  $W$ , each of the  $L$ -functions has an Euler product expansion. Thus we have the following result.

LEMMA 2.1. Write  $V = GH$  where  $G$  and  $H$  are monic, relatively prime polynomials over  $GF(q)$  with  $G$  primitive and  $H$  a  $(q-1)$ th power. Then

$$(2.6) \quad L(t, V) = L(t, G) \prod_{v|H} (1 - \tau(R(G, v)) t^{\deg v}),$$

$$(2.6a) \quad L_1(t, V) = L_1(t, G) \prod_{v|H} (1 - \psi(\alpha(v)) \tau(R(G, v)) t^{\deg v}),$$

and

$$(2.6b) \quad L_2(t, V) = L_2(t, G) \prod_{v|H} (1 - \psi(\beta(v))\tau(R(G, v))t^{\deg v}) .$$

The next lemma evaluates certain generating functions defined in terms of the function  $L$  (but not  $L_1$  or  $L_2$ ).

LEMMA 2.2. For all integers  $a, b > 0$ ,

$$(2.7) \quad \sum_W \tau(W^a(0)W^b(1))L(t, W^{q-1})z^{\deg W} = \begin{cases} \frac{1 + \tau(-1)^a J(a, b)z}{(1-qt)(1 + \tau(-1)^a J(a, b)zt)}, & \text{if } a \not\equiv 0 \pmod{q-1} \\ & \text{or } b \not\equiv 0 \pmod{q-1}, \\ \frac{(1-z)^2(1-qzt)}{(1-qt)(1-qz)(1-zt)^2}, & \text{if } a \equiv b \equiv 0 \pmod{q-1}, \end{cases}$$

$$(2.7a) \quad \sum_W \psi(\alpha(W^b))\tau(W(0)^a)L(t, W^{q-1})z^{\deg W} = \frac{1 + \bar{\tau}^a(b)G(a)z}{(1-qt)(1 + \bar{\tau}^a(b)G(a)zt)},$$

and

$$(2.7b) \quad \sum_W \psi(\beta(W^b))L(t, W^{q-1})z^{\deg W} = \frac{1 + \phi(2b)G((q-1)/2)z}{(1-qt)(1 + \phi(2b)G((q-1)/2)zt)},$$

where in each sum,  $W$  ranges over all monic polynomials over  $GF(q)$  and  $\alpha, \beta$  are as defined in (2.3).

*Proof.* Fix monic  $V = V(x)$  and let  $w$  range over monic irreducibles over  $GF(q)$ . By (2.6),

$$\begin{aligned} & \sum_W \tau(R(V, W))L(t, W^{q-1})z^{\deg W} \\ &= L(t, 1) \sum_W z^{\deg W} \tau(R(V, W)) \prod_{w|W} (1 - t^{\deg w}) \\ &= L(t, 1) \sum_W \prod_{w|W} \{(1 - t^{\deg w}) (\tau(R(V, w))z^{\deg w})^{\text{ord}_w W}\} \\ &= L(t, 1) \prod_w \left\{ 1 + (1 - t^{\deg w}) \sum_{m=1}^{\infty} (\tau(R(V, w))z^{\deg w})^m \right\} \\ &= L(t, 1) \prod_w \frac{1 - \tau(R(V, w)) (zt)^{\deg w}}{1 - \tau(R(V, w))z^{\deg w}} = \frac{L(t, 1)L(z, V)}{L(zt, V)}. \end{aligned}$$

Taking  $V = x^a(x-1)^b$ , we easily deduce (2.7). The proofs of (2.7a) and (2.7b) are similar.  $\square$

It is shown in [1, Prop. 2.1] that if  $V$  is primitive of degree  $> 0$ , then  $L(t, V)$  is a polynomial in  $t$  of degree  $(\deg F - 1)$  with leading coefficient

$$(2.8) \quad \varepsilon(V) = \sigma(F)\tau(R(V, F'))G^*(\deg V)^{-1} \prod_{v|F} G^*(\text{ord}_v V)^{\deg v},$$

where

$$G^*(a) := q/G(-a).$$

By (2.6), if  $V$  is a  $(q-1)$ th power, then

$$L(t, V) = (1 - qt)^{-1} \prod_{v|V} (1 - t^{\deg v}),$$

but otherwise  $L(t, V)$  is a polynomial of degree  $(\deg F - 1)$ . The following lemma shows that for all  $V$ ,  $L_1(t, V)$  and  $L_2(t, V)$  are polynomials of degrees  $\deg F$  and  $\deg F + 1$ , respectively. Moreover, for primitive  $V \neq 1$ , the coefficient  $\varepsilon_1(V)$  of  $t^{\deg F}$  in  $L_1(t, V)$  and the coefficient  $\varepsilon_2(V)$  of  $t^{1+\deg F}$  in  $L_2(t, V)$  are given explicitly.

**LEMMA 2.3.** *For each monic polynomial  $V$  over  $GF(q)$ ,  $L_1(t, V)$  and  $L_2(t, V)$  are polynomials in  $t$  of degrees  $\deg F$  and  $1 + \deg F$ , respectively. If moreover  $V \neq 1$  is primitive, the leading coefficients of  $L_1(t, V)$  and  $L_2(t, V)$  are given by*

$$(2.8a) \quad \varepsilon_1(V) = \psi(\alpha(F))\sigma(F)\tau(R(V, -F')) \prod_{v|F} G^*(\text{ord}_v V)^{\deg v},$$

and

$$(2.8b) \quad \varepsilon_2(V) = \phi(2)G((q-1)/2)\psi(\beta(F))\sigma(F)\tau(R(V, F')) \prod_{v|F} G^*(\text{ord}_v V)^{\deg v},$$

respectively, where  $G^*(a) = q/G(-a)$ .

*Proof.* Fix an integer  $m > \deg F$  and fix  $\alpha \in GF(q)$ . Since  $m > \deg F$ , it is not hard to see that the monic polynomials  $W$  over  $GF(q)$  of degree  $m$  with  $\alpha(W) = \alpha$  run through each residue class modulo  $F$  exactly  $q^{m-1-\deg F}$  times. Since  $R(V, W)$  depends only on the residue class of  $W$  modulo  $F$ , the coefficient of  $t^m$  in  $L_1(t, V)$  thus equals

$$\begin{aligned} & \sum_{\substack{W \text{ monic} \\ \deg W = m}} \psi(\alpha(W))\tau(R(V, W)) \\ &= q^{m-1-\deg F} \sum_{\substack{U \\ \deg U < \deg F}} \tau(R(V, U)) \sum_{\alpha \in GF(q)} \psi(\alpha) = 0. \end{aligned}$$

Therefore  $L_1(t, V)$  is a polynomial of degree  $\leq \deg F$ . Similar reasoning with  $\beta(W)$  in place of  $\alpha(W)$  shows that  $L_2(t, V)$  is a polynomial of degree  $\leq 1 + \deg F$ . In view of (2.5), (2.6a) and (2.6b), it remains to prove (2.8a) and (2.8b) for primitive  $V \neq 1$ .

To prove (2.8a), consider the double sum

$$(2.9) \quad \mu_1 := \sum_U \sum_W \psi \left( - \operatorname{Res}_\infty \frac{U(x)W(x)}{F(x)} \right) \psi(\alpha(W))\bar{\tau}(R(V, U)),$$

where  $W = W(x)$  ranges over monic polynomials of degree  $D := \deg F$  over  $GF(q)$  and  $U = U(x)$  ranges over nonzero polynomials of degree  $< D$  over  $GF(q)$ . Write  $k = \deg U$ ,

$$(2.10) \quad W(x) = w_D x^D + w_{D-1} x^{D-1} + \dots + w_0, \quad (w_D = 1),$$

and

$$(2.11) \quad \frac{x^k U(1/x)}{x^D F(1/x)} = a_0 + a_1 x + a_2 x^2 + \dots.$$

Note that  $a_0 \neq 0$  is the leading coefficient of  $U(x)$ . We have

$$(2.12) \quad \psi \left( \alpha(W) - \operatorname{Res}_\infty \frac{UW}{F} \right) = \psi \left( w_{D-1} + \sum_{i=0}^{k+1} a_{k+1-i} w_{D-i} \right).$$

For fixed  $U$ , the sum over  $W$  in (2.9) thus vanishes unless  $U(x) = -1$ . When  $U(x) = -1$ , each member of (2.12) equals  $\psi(a_1) = \psi(\alpha(F))$ . Therefore

$$(2.13) \quad \mu_1 = q^{\deg F} \tau(-1)^{\deg V} \psi(\alpha(F)).$$

On the other hand, by the proof of the last formula in [1, §2] (here primitivity is used), we have

$$(2.14) \quad \mu_1 = \varepsilon_1(V) \sigma(F) \bar{\tau}(R(V, F')) \prod_{v|F} G(-\operatorname{ord}_v V)^{\deg v}.$$

Comparison of (2.13) and (2.14) yields (2.8a).

To prove (2.8b), consider the double sum

$$(2.15) \quad \mu_2 := \sum_U \sum_Y \psi \left( - \operatorname{Res}_\infty \frac{U(x) Y(x)}{F(x)} \right) \psi(\beta(Y)) \bar{\tau}(R(V, U))$$

where  $Y$  ranges over monic polynomials of degree  $D + 1$  over  $GF(q)$  (with  $D = \deg F$ ) and  $U$  ranges over nonzero polynomials of degree  $< D$  over  $GF(q)$ . Write  $k = \deg U$  and

$$(2.16) \quad Y(x) = y_{D+1}x^{D+1} + y_Dx^D + \cdots + y_0, \quad (y_{D+1} = 1).$$

In the notation of (2.11),

$$(2.17) \quad \psi \left( \beta(Y) - \operatorname{Res}_\infty \frac{UY}{F} \right) = \psi \left( y_D^2/2 - y_{D-1} + \sum_{i=0}^{k+2} a_{k+2-i} y_{D+1-i} \right).$$

For fixed  $U$ , the sum over  $Y$  in (2.15) vanishes unless  $U(x) = 1$ . When  $U(x) = 1$ , each member of (2.17) equals  $\psi(a_2 + a_1 y_D + y_D^2/2)$  with

$$a_1 = -\alpha(F), \quad a_2 = \alpha(F)^2/2 + \beta(F).$$

Therefore

$$(2.18) \quad \mu_2 = q^D \psi(\beta(F)) \sum_{y \in GF(q)} \psi(y^2/2) = q^D \psi(\beta(F)) \phi(2) G((q-1)/2).$$

On the other hand, by the proof of the last formula in [1, §2], we have

$$(2.19) \quad \mu_2 = \varepsilon_2(V) \sigma(F) \bar{\tau}(R(V, F')) \prod_{v|F} G(-\operatorname{ord}_v V)^{\deg v}.$$

Comparison of (2.18) and (2.19) yields (2.8b).

### §3. PROOF OF THEOREMS 1.1, 1.1a, 1.1b

Let  $d$  denote the order of  $\tau^c$ . The following lemma gives useful formulas for  $P_n(a, b, c)$ ,  $P_n(a, c)$ , and  $P_n(c)$  in the case  $d | n$ . The proof of (3.1b) is elementary but for (3.1) and (3.1a) we require the Hasse-Davenport product formula [7, (7)].

LEMMA 3.1. *Let  $d$  be the smallest positive integer such that  $cd \equiv 0 \pmod{q-1}$ . If  $d | n$ , then*