Exponential sums

The estimate of Hasse-Davenport-Weil.

Peter Roquette (Heidelberg) [1])
July 23, 2003

1 Statement of main result

Let p be a prime number. We consider *exponential sums* which are expressions of the form

$$S_f = \sum_{a \bmod p} e^{\frac{2\pi i\, f(a)}{p}}$$

where $f(x) \in \mathbb{Z}[x]$ is a polynomial with integer coefficients. More generally, instead of the prime field $\mathbb{Z}/p$ we may work over any finite field K with $q = p^k$ elements. Let $\mathrm{tr} : K \to \mathbb{Z}/p$ denote the trace operator from K to its prime field. Then, an *exponential sum* over K is any expression of the form

$$S_f = \sum_{a \in K} e^{\frac{2\pi i \,\mathrm{tr}\, f(a)}{p}}$$

where $f(x) \in K[x]$ is a polynomial. In order to simplify notation, we put

$$\chi(a) = e^{\frac{2\pi i \,\mathrm{tr}\,(a)}{p}} \qquad (a \in K)\,. \tag{1}$$

This is the *canonical character* $\chi : K \to W_p$ from the additive group of K onto the multiplicative group W_p of p-th roots of unity in the field of complex numbers. Now the exponential sum as above can be written in the form

$$S_f = \sum_{a \in K} \chi\, f(a)\,. \tag{2}$$

[1]) These notes are meant as reading material for an introductory course on algebraic function fields. They contain proofs and references for some part of my lectures at the Escola de Algebra in Rio de Janeiro, July 1996. The notations here, however, may not always be the same as are used in the lecture. – The present version contains some minor corrections of the published version.

Our aim is to derive an upper bound for the absolute value $|S_f|$ of such an exponential sum.

Every summand of S_f is a complex number of absolute value 1. Since there are q summands we have the trivial estimate

$$|S_f| \leq q\,. \tag{3}$$

For some polynomials $f(x)$ we have equality here. For instance, if $f(x) = c$ is a constant polynomial then $\chi\, f(a) = \chi(c)$ for every $a \in K$ and hence: $S_f = q\chi(c)$, $|S_f| = q$. Another instance occurs when $f(x)$ is of the form $f(x) = g(x)^p - g(x)$ for some polynomial $g(x) \in K[x]$. Then for each $a \in K$ we have $\operatorname{tr} g(a)^p = \operatorname{tr} g(a)$, hence $\operatorname{tr} f(a) = 0$, $\chi\, f(a) = 1$. Thus $S_f = q$.

In both these instances the degree d of $f(x)$ is divisible by p. Now we claim:

Theorem 1 *Suppose that the degree d of $f(x)$ is not divisible by p. Then the exponential sum* (2) *admits the estimate*

$$|S_f| \leq (d-1)\sqrt{q}\,. \tag{4}$$

Of course, this is a proper improvement against (3) only if $d \leq \sqrt{q}$. The essential point of Theorem 1 is that *for large q* this estimate, involving only the square root, is of much smaller order of magnitude than the trivial estimate q. This is of great importance in various applications, not only in coding theory but also in number theory. It can be shown that the exponent $\frac{1}{2}$, which occurs in the square root, is best possible for this problem in its order of magnitude.

Remark. If $f(x)$ is of the form

$$f(x) = f_1(x) + g(x)^p - g(x) \tag{5}$$

then $\operatorname{tr} f(a) = \operatorname{tr} f_1(a)$ and hence $S_f = S_{f_1}$. Now, it is easily verified [2]) that every polynomial $f(x) \in K[x]$ can be written in the form (5) such that

$$\deg f_1(x) \leq \deg f(x)$$

and that the following alternatives hold:

$$\begin{array}{rrcl} \textit{either} & \deg f_1(x) & \not\equiv & 0 \bmod p \\ \textit{or} & \deg f_1(x) & = & 0\,. \end{array}$$

[2]) See e.g., [S] p.114. (Letters in brackets refer to the bibliography at the end of these notes.)

In the first case we see that the estimate (4) of Theorem 1 for $f_1(x)$ implies the same for $f(x)$. In the second case $f_1(x) = c \in K$. Thus the only exceptions to (4) are the polynomials of the form

$$f(x) = c + g(x)^p - g(x)$$

and for these we have seen that $|S_f| = q$.

In the following we shall assume throughout that the degree of $f(x)$ is

$$d \not\equiv 0 \bmod p\,.$$

We leave it to the reader to find out which part of our statements remain valid for arbitrary polynomials.

□

The case of degree $d = 1$ is easily dealt with. Namely, we then have $f(x) = c_0 + c_1 x$ with $c_1 \neq 0$. If a ranges over the elements in K then $c_0 + c_1 a$ ranges also over all the elements in K; hence

$$S_f = \sum_{a \in K} \chi(c_0 + c_1 a) = \sum_{a \in K} \chi(a) = 0$$

because χ is a *nontrivial* character of the additive group of K.

In the next sections we shall prepare the way which will enable us to deal with arbitrary degree $d \not\equiv 0 \bmod p$. Our presentation here follows essentially that given by HASSE [H]. We shall have to use several facts on algebraic function fields; these can all be found in STICHTENOTH's book [S].

2 The divisor character χ_f and its L-series

We work in the rational function field $F = K(x)$. From [S] Chap. I we recall the notions of *place* and *divisor* of F. There are $q + 1$ places of degree 1 of F, and they correspond $1 - 1$ to the q elements $a \in K$ and to ∞. We use the notations P_a and P_∞ respectively. If $a \in K$ then P_a is the zero of the polynomial $x - a$. And P_∞ is the pole of x, which equals the zero of x^{-1}.

The places $P \neq P_\infty$ of F correspond $1 - 1$ to the irreducible monic polynomials $h(x) \in K[x]$, such that P is the zero divisor of $h(x)$. We use the notation $h_P(x)$ to indicate that this polynomial corresponds to P. The residue field of P is $F_P = K(\alpha)$ where α is a root of $h_P(x)$. The degree of P equals the polynomial degree of $h_P(x)$. If $a \in K$ then $h_{P_a}(x) = x - a$.

We consider divisors D of F which do not contain P_∞ in their support. Every such divisor is of the form

$$D = \sum_{P \neq P_\infty} n_P \cdot P \tag{6}$$

where the multiplicities n_P are integers, only finitely many of which are $\neq 0$. These divisors form a group $\mathfrak{D}_f$, a subgroup of the group $\mathfrak{D}$ of all divisors of F. The notation $\mathfrak{D}_f$ indicates that the pole of f, namely P_∞, is excluded.

First assume that D is positive; this means that $n_P \geq 0$ for all multiplicities n_P of D. We write $D \geq 0$. We put

$$h_D(x) = \prod_{P \neq P_\infty} h_P(x)^{n_P} ;$$

this is a monic polynomial in $K[x]$, called the *characteristic polynomial* of D. Its degree is

$$n = \sum_{P \neq P_\infty} n_P \deg P = \deg D .$$

We decompose $h_D(x)$ into linear factors:

$$h_D(x) = \prod_{1 \leq i \leq n} (x - \alpha_i) . \tag{7}$$

The roots α_i [3]) are contained in some algebraic extension of K. For any α_i, all its conjugates over K are also roots of $h_D(x)$, with the same multiplicity as α_i itself. Hence the following definition yields an element $\partial_f(D) \in K$:

$$\partial_f(D) = \sum_{1 \leq i \leq n} f(\alpha_i) . \tag{8}$$

If $D_1, D_2 \geq 0$ are two positive divisors then $h_{D_1+D_2} = h_{D_1} h_{D_2}$ and hence

$$\partial_f(D_1 + D_2) = \partial_f(D_1) + \partial_f(D_2) .$$

If $D \in \mathfrak{D}_f$ is an arbitrary divisor, not necessarily positive, then we write $D = D_1 - D_2$ as the difference of two positive divisors and define

$$\partial_f(D) = \partial_f(D_1) - \partial_f(D_2) .$$

Indeed this is well defined. We thus obtain an additive homomorphism

$$\partial_f : \mathfrak{D}_f \to K$$

from the divisor group $\mathfrak{D}_f$ to the additive group of K. The notation ∂_f has been chosen in order to indicate that, as we shall see later, this homomorphism can also be defined by suitable *differentiation* in the field F.

---

[3]) From now on we shall use the letter i as a running index. We shall not have occasion any more to interpret $i = \sqrt{-1}$ as in section 1.

Combined with the canonical character χ we obtain a character $D \mapsto \chi\,\partial_f(D)$ from $\mathfrak{D}_f$ to the multiplicative group W_p of p-th roots of unity. This character is denoted by

$$\chi_f : \mathfrak{D}_f \to W_p\,.$$

If $D = P_a$ with $a \in K$ then by definition,

$$\partial_f(P_a) = f(a) \tag{9}$$

and hence

$$\chi_f(P_a) = \chi\, f(a)\,. \tag{10}$$

Now let t be a complex variable and consider the power series

$$L(t\,|\,\chi_f) = \sum_{D\geq 0} \chi_f(D)\cdot t^{\deg D} = 1 + \sum_{n\geq 1}\left(\sum_{\substack{\deg D = n\\ D\geq 0}} \chi_f(D)\right)\cdot t^n\,. \tag{11}$$

where D ranges over the positive divisors in $\mathfrak{D}_f$. The coefficient of the first power t^1 can be described as follows: The positive divisors $D \in \mathfrak{D}_f$ of degree 1 are precisely the places P_a of degree 1, corresponding to the elements $a \in K$. For those we have (10) and hence the coefficient of t^1 in (11) equals $\sum_{a\in K} \chi f(a)$. This is precisely the exponential sum S_f from (2) which we wish to estimate. Thus,

$$L(t\,|\,\chi_f) = 1 + S_f\cdot t + \cdots \tag{12}$$

where the dots indicate terms of higher degree in t. This fact, namely that S_f appears as the coefficient of the first term of $L(t\,|\,\chi_f)$, will explain the appearance of this L-series for the proof of Theorem 1.

The following two theorems govern the behavior of $L(t\,|\,\chi_f)$.

Theorem 2 *Assume $d \not\equiv 0 \bmod p$. Then the L-series $L(t\,|\,\chi_f)$ is in fact a polynomial in the complex variable t, of degree $d-1$.*

Accordingly, let us decompose $L(t\,|\,\chi_f)$ into linear factors:

$$L(t\,|\,\chi_f) = \prod_{1\leq i\leq d-1}(1-\omega_i t)$$

where the ω_i are certain complex numbers, the inverse roots of $L(t\,|\,\chi_f)$. We see that the coefficient of t^1 is the negative sum of these ω_i. Comparing with (12) we conclude:

$$S_f = -\sum_{1\leq i\leq d-1}\omega_i\,. \tag{13}$$

Now we have, in addition to Theorem 2:

Theorem 3 *Each root ρ_i of the polynomial $L(t\,|\,\chi_f)$ is of absolute value $|\rho_i| = \sqrt{q^{-1}}$. Consequently the inverse roots $\omega_i = \rho_i^{-1}$ are of absolute value $|\omega_i| = \sqrt{q}$.*

Therefore from (13) it follows:

$$|S_f| \leq (d-1)\sqrt{q}$$

which is the content of Theorem 1. Note that by Theorem 2 the sum in (13) has at most $d-1$ terms ω_i ; if $d \not\equiv 0 \bmod p$ then the number of terms in (13) is precisely $d-1$.

We have seen that Theorem 1 is an immediate consequence of Theorem 2 and Theorem 3. In the following, we shall first discuss the proof Theorem 2, then turn to Theorem 3.

3 The conductor of χ_f

By definition, χ_f is obtained by first applying the divisor homomorphism $\partial_f : \mathfrak{D}_f \to K$, then applying the canonical character $\chi : K \to W_p$. Accordingly we first discuss the properties of the divisor homomorphism ∂_f. Thereafter we shall draw the consequences for χ_f.

Consider the valuation ring $\mathcal{O}_\infty$ of P_∞; it consists of all $h \in F$ with $v_\infty(h) \geq 0$. Recall that, by definition, the valuation v_∞ is the negative degree function. Two elements $h, h' \in \mathcal{O}_\infty$ are said to be *congruent modulo* $(d+1)P_\infty$ if

$$v_\infty(h - h') \geq d+1\,.$$

If this is the case then we write

$$h \equiv h' \bmod (d+1)P_\infty\,.$$

These congruence classes form a ring, the residue class ring of $\mathcal{O}_\infty$ modulo the $(d+1)$-th power of its maximal ideal.

The group of units of $\mathcal{O}_\infty$ is denoted by $\mathcal{O}_\infty^\times$; it consists of those $h \in F$ for which $v_\infty(h) = 0$. This means that the principal divisor (h) does not contain P_∞ in its support, i.e., $(h) \in \mathfrak{D}_f$.

Two divisors $D, D' \in \mathfrak{D}_f$ are said to be *equivalent modulo* $(d+1)P_\infty$ if

$$D - D' = (h) \tag{14}$$

is the principal divisor of an element $h \in \mathcal{O}_\infty$ which satisfies

$$h \equiv 1 \bmod (d+1)P_\infty\,. \tag{15}$$

(This implies $h \in \mathcal{O}_\infty^\times$.) If this is the case then we write

$$D \sim D' \bmod (d+1)P_\infty \,.$$

The corresponding divisor classes are called *ray classes* modulo $(d+1)P_\infty$.

Our first aim is to prove that $\partial_f(D)$ depends only on the ray class of D modulo $(d+1)P_\infty$. That is, we have to show that $\partial_f(D) = 0$ if $D \sim 0 \bmod (d+1)P_\infty$. To this end we will give another description of how to compute $\partial_f(D)$.

The differential [4]) $\dfrac{\mathrm{d}h}{h}$ is called the *logarithmic differential* of h, and it is denoted by $\mathrm{dlog}\, h$. We note the homomorphic property:

$$\mathrm{dlog}\,(h_1 h_2) = \mathrm{dlog}\, h_1 + \mathrm{dlog}\, h_2 \,. \tag{16}$$

If D is any divisor in $\mathfrak{D}_f$, say of degree n, then $D - nP_\infty$ is of degree 0 and hence a principal divisor:

$$D - nP_\infty = (h)$$

for some $0 \neq h \in F$ which is uniquely determined up to a constant factor. We write this relation in the form

$$D = (h)_f \tag{17}$$

which says that the principal divisor of h represents D except at the pole of f (which is P_∞).

Lemma 4 *Let $D \in \mathfrak{D}_f$ be represented by $h \in F$ in the sense* (17) *as explained above. Then*

$$\partial_f(D) = -\mathrm{res}_\infty(f \cdot \mathrm{dlog}\, h) \tag{18}$$

where res_∞ *denotes the residue at* P_∞ *.*

Proof:

(i) If D is represented by h and by h' then $h' = c \cdot h$ with $c \in K^\times$. We note that $\mathrm{dlog}\,(c \cdot h) = \mathrm{dlog}\, h$; thus the right hand side of (18) does not change if we replace h by $c \cdot h$. In other words: It is clear from the start that the right hand side of (18) depends on D only and not on the choice of the function h which represents D.

---

[4]) As for the notion and properties of differentials and their residues we refer to [S] Ch. IV.

(ii) Every divisor D is a linear combination, with integer coefficients, of prime divisors. Because of the homomorphic property (16) we conclude: it is sufficient to prove (18) in the case when $D = P$ is a prime divisor. For simplicity, let us first discuss the case when $P = P_a$ is of degree 1, hence h can be taken to be the linear polynomial $h = x - a$. By (9) we have $\partial_f(P_a) = f(a)$.

For the computation of the residue at P_∞ we have to expand all functions involved into Laurent series with respect to a prime element at P_∞. We take $u = x^{-1}$ as prime element and compute

$$\begin{aligned} \mathrm{dlog}\,(x-a) &= \frac{\mathrm{d}x}{x-a} = \frac{x^{-1}\mathrm{d}x}{1-ax^{-1}} = \frac{-u^{-1}\mathrm{d}u}{1-au} \\ &= -\sum_{0\le\nu<\infty} a^\nu u^\nu \mathrm{dlog}\, u\,. \end{aligned}$$

We write

$$f(x) = \sum_{0\le j\le d} c_j x^j = \sum_{0\le j\le d} c_j u^{-j}$$

and obtain

$$-f\cdot\mathrm{dlog}\,(x-a) = \sum_{0\le j\le d}\sum_{0\le\nu<\infty} c_j a^\nu u^{\nu-j}\mathrm{dlog}\, u\,.$$

By definition, $\mathrm{dlog}\, u = u^{-1}\mathrm{d}u$ has a pole of order 1 at P_∞, with residue $= 1$. Hence we see that the residue of the left hand side is obtained as the coefficient of u^0 in the above expansion, i.e., the sum of the terms with $\nu = j$:

$$-\mathrm{res}_\infty f\cdot\mathrm{dlog}\,(x-a) = \sum_j c_j a^j = f(a)\,. \tag{19}$$

(iii) Now, if $D = P$ is a prime divisor of degree $n > 1$ then we decompose its characteristic polynomial $h_P(x)$ into linear factors as in (7). The roots α_i are contained in an algebraic extension of K, and $\partial_f(P)$ is given by (8):

$$h_P(x) = \prod_{1\le i\le n}(x-\alpha_i)\,, \qquad \partial_f(P) = \sum_{1\le i\le n} f(\alpha_i)\,.$$

Accordingly, using the result of the computation (19) for each factor:

$$\begin{aligned} -\mathrm{res}_\infty f\cdot\mathrm{dlog}\, h_D(x) &= -\sum_{1\le i\le n}\mathrm{res}_\infty f\cdot\mathrm{dlog}\,(x-\alpha_i) \\ &= \sum_{1\le i\le n} f(\alpha_i) = \partial_f(P)\,. \end{aligned}$$

□

Proposition 5 *If $D \sim 0 \bmod (d+1)P_\infty$ then $\partial_f(D) = 0$. Hence the homomorphism $\partial_f : \mathfrak{D}_f \to K$ depends only on the ray classes of $\mathfrak{D}_f$ modulo $(d+1)P_\infty$. If $d \not\equiv 0 \bmod p$ then the number $d+1$ is minimal with the above property. In fact, ∂_f induces a surjection from the group of divisors $D \sim 0 \bmod dP_\infty$ onto K.*

Proof:

Suppose that $D \sim 0 \bmod dP_\infty$. Then $D = (h)$ with $h \equiv 1 \bmod dP_\infty$. As above, we use $u = x^{-1}$ as a prime element at P_∞; the corresponding expansion of h is of the form

$$h = 1 + au^d + \cdots \qquad\qquad (\text{at } P_\infty) \tag{20}$$

with $a \in K$. The dots indicate terms of higher order. Differentiation yields

$$\mathrm{d}h = dau^{d-1}\mathrm{d}u + \cdots$$

Multiplying with $h^{-1} \equiv 1 \bmod dP_\infty$:

$$\mathrm{dlog}\, h = dau^{d-1}\mathrm{d}u + \cdots = dau^d \mathrm{dlog}\, u + \ldots$$

Hence

$$\begin{aligned} f \cdot \mathrm{dlog}\, h &= \left(c_d u^{-d} + c_{d-1}u^{-d+1} + \ldots + c_0\right) \cdot \left(dau^d\, \mathrm{dlog}\, u + \cdots\right) \\ &= c_d da\, \mathrm{dlog}\, u + \cdots . \end{aligned}$$

Here, the dots represent differentials of order ≥ 0, without residue. We obtain in view of Lemma 4

$$\partial_f(D) = -c_d \cdot d \cdot a\,. \tag{21}$$

This holds for every divisor $D \sim 0 \bmod dP_\infty$.

If $D \sim 0 \bmod (d+1)P_\infty$ then $a = 0$ and hence $\partial_f(D) = 0$.

Now, if $d \not\equiv 0 \bmod p$ then $c_d \neq 0$. Consequently, $\partial_f(D) = 0$ *only if* $a = 0$ which means $D \sim 0 \bmod (d+1)P_\infty$. Moreover, *every* element $a \in K$ belongs to some divisor $D \sim 0 \bmod dP_\infty$, in the sense of (20). For instance we can take D to be the principal divisor of the function

$$h = 1 + au^d = \frac{x^d + a}{x^d}\,.$$

If a ranges over K then, by (21), we see that $\partial_f(D)$ ranges over K too.

□

Next we consider the character $\chi_f = \chi \circ \partial_f$. Since χ is nontrivial on K we obtain from Proposition 5 the following proposition which will turn out to be the key to Theorem 2.

Proposition 6 *As above, d denotes the degree of the polynomial $f(x)$. The character $\chi_f : \mathfrak{D} \to W_p$ is a ray character modulo $(d+1)P_\infty$, which means that $\chi_f(D)$ depends only on the ray class of D modulo $(d+1)P_\infty$. Moreover, $d+1$ is the minimal integer with this property. In fact, χ_f induces a surjection from the group of divisors $D \sim 0 \bmod dP_\infty$ onto W_p.*

Because of the minimality property mentioned, the divisor $(d+1)P_\infty$ is called the *conductor* of the character χ_f. This terminology is borrowed from number theory where it is used in similar situations for divisor characters.

4 The L-series as a polynomial

If two divisors $D, D' \in \mathfrak{D}_f$ are equivalent modulo $(d+1)P_\infty$ then they have the same degree: This follows from the definition in section 3 since $D - D'$ is a principal divisor, hence of degree 0. Consequently we can speak of "ray classes modulo $(d+1)P_\infty$ of a given degree".

Lemma 7 *For each n there are q^d ray classes modulo $(d+1)P_\infty$ of degree n. If $n \geq d$ then every such ray class contains a positive divisor and the number of positive divisors in each ray class is q^{n-d}.*

Proof:

(i) Let $D \in \mathfrak{D}_f$ be of degree n, and let $D = (h)_f$. As in the foregoing section we consider the expansion of h at P_∞ with respect to the prime element $u = x^{-1}$. We have $v_\infty(h) = -\deg h = -\deg D = -n$, hence this expansion is of the form $h = cu^{-n} + \cdots$ with $0 \neq c \in K$. After multiplication of h with c^{-1} we may assume that $c = 1$. We write the expansion of h in the form

$$h = u^{-n}(1 + a_1 u + a_2 u^2 + \cdots) \qquad (\text{at } P_\infty)\,. \tag{22}$$

Let D' be a second divisor of degree n, with representing function h' and expansion

$$h' = u^{-n}(1 + a_1' u + a_2' u^2 + \cdots) \qquad (\text{at } P_\infty)\,.$$

According to the definition, we have $D \sim D' \bmod (d+1)P_\infty$ if and only if $\dfrac{h}{h'} \equiv 1 \bmod (d+1)P_\infty$, which is to say that

$$1 + a_1 u + a_2 u^2 + \cdots \equiv 1 + a_1' u + a_2' u^2 + \cdots \bmod (d+1)P_\infty\,.$$

This in turn means

$$a_i = a'_i \qquad (1 \le i \le d)\,.$$

Now, *every* vector $(a_1, \dots a_d)$ over K belongs to a ray class of degree n in the above sense, namely to the ray class of the divisor D which is represented by

$$h = u^{-n}(1 + a_1 u + \cdots + a_d u^d) = x^n + a_1 x^{n-1} + \cdots + a_d x^{n-d}\,. \qquad (23)$$

Thus there is a $1-1$ correspondence between the ray classes modulo $(d+1)P_\infty$ of degree n, and the vectors in the d-dimensional vector space K^d.

Since K has order q there are precisely q^d vectors in K^d. We conclude that there are q^d ray classes modulo $(d+1)P_\infty$ of given degree n, as contended.

(ii) If $n \ge d$ then the function h in (23) is a monic polynomial in $K[x]$, hence h is the characteristic polynomial of a positive divisor, hence $D \ge 0$.

(iii) Let $n \ge d$. The positive divisors D of degree n correspond $1-1$ to their characteristic polynomials $h_D(x)$, which are monic polynomials of degree n:

$$h_D(x) = x^n + a_1 x^{n-1} + \cdots + a_n$$

We have seen in (i) that the ray class of D modulo $(d+1)P_\infty$ is uniquely characterized by the vector $(a_1, \dots, a_d)$ of the first d coefficients. If we fix this vector then there are precisely q^{n-d} vectors of the form $(a_{d+1}, \dots, a_n)$ each of which belongs to a positive divisor of the same ray class.

□

Now we are able to show:

Proposition 8 *If $n \ge d$ then $\sum_{\substack{\deg D = n \\ D \ge 0}} \chi_f(D) = 0$. Consequently, the L-series $L(t \,|\, \chi_f)$ as defined in (11) is a polynomial in t of degree $\le d-1$.*

(Later it will turn out that the degree is precisely $d-1$.)

Proof:

By Proposition 6 the character value $\chi_f(D)$ depends only on the ray class of D modulo $(d+1)P_\infty$. Let $n \ge d$. By Lemma 7 each ray class of degree n contains q^{n-d} positive divisors. We choose a set $\mathfrak{R}_n$ of representatives of the ray classes modulo $(d+1)P_\infty$ of degree n. Then

$$\sum_{\substack{\deg D = n \\ D \ge 0}} \chi_f(D) = q^{n-d} \sum_{D \in \mathfrak{R}_n} \chi_f(D)\,.$$

Let $A \in \mathfrak{D}_f$ be a fixed, auxiliary divisor of degree n. We subtract A from each divisor $D \in \mathfrak{R}_n$ and obtain a system of representatives $\mathfrak{R}_0 = \mathfrak{R}_n - A$ of the ray classes modulo $(d+1)P_\infty$ of degree 0. We put $D - A = D_0$, so that $\chi_f(D) = \chi_f(A)\chi_f(D_0)$, and we compute

$$\sum_{D \in \mathfrak{R}_n} \chi_f(D) = \chi_f(A) \sum_{D_0 \in \mathfrak{R}_0} \chi_f(D_0)\,.$$

According to Lemma 7 the ray classes modulo $(d+1)P_\infty$ of degree 0 form a *finite* group, of order q^d. By Proposition 6 the character χ_f induces a *nontrivial* character on that group. Consequently,

$$\sum_{D_0 \in \mathfrak{R}_0} \chi_f(D_0) = 0$$

which proves our contention.

□

Since $d \not\equiv 0 \bmod p$ it will turn out that the degree of the polynomial $L(t \,|\, \chi_f)$ is precisely $d-1$, in accordance with the contention of Theorem 2 .

5 Artin-Schreier extension of $K(x)$

Let P be a prime divisor of $F = K(x)$, and assume $P \neq P_\infty$. Let F_P denote the residue field. We have $F_P = K(\alpha)$ where α is a root of the characteristic polynomial $h_P(x)$. In this situation we claim:

Proposition 9 *$\chi_f(P) = 1$ if and only if there exists $\beta \in F_P$ such that $\beta^p - \beta = f(\alpha)$.*

Proof:

By definition (1), the canonical character χ is composed of the trace map $\mathrm{tr}_K : K \to \mathbb{Z}/p$ [5]) and of the isomorphism $\mathbb{Z}/p \approx W_p$ given by the exponential function. Hence

$$\chi_f(P) = \chi\,\partial_f(P) = 1 \qquad \Longleftrightarrow \qquad \mathrm{tr}_K\,\partial_f(P) = 0\,.$$

Accordingly we will show that $\mathrm{tr}_K\,\partial_f(P) = 0$ if and only if the condition as given in Proposition 9 is satisfied.

---

[5]) We write tr_K if we wish to indicate the field K on which this trace is defined.

The characteristic polynomial $h_P(x)$ is irreducible over K and hence its roots are precisely the conjugates α^{q^i} over K. Here, i ranges from 0 to $n-1$ where $n = \deg P = [F_P : K]$. It follows

$$\partial_f(P) = \sum_{0 \le i \le n-1} f(\alpha^{q^i}) = \sum_{0 \le i \le n-1} f(\alpha)^{q^i} = \mathrm{tr}_P f(\alpha)$$

where $\mathrm{tr}_P : F_P \to K$ denotes the relative trace map from the residue field F_P. The so-called "transitivity rule" for the trace says that $\mathrm{tr}_K \circ \mathrm{tr}_P = \mathrm{tr}_{F_P}$, and so we conclude

$$\mathrm{tr}_K\, \partial_f(P) = \mathrm{tr}_{F_P}\, f(\alpha)\,.$$

Now our contention is evident from the following well known statement on the trace function of finite fields:

Let L be any finite field and $z \in L$. Then we have $\mathrm{tr}_L(z) = 0$ if and only if there exists $\beta \in L$ such that $\beta^p - \beta = z$.

Indeed, since the trace map $\mathrm{tr}_L : L \to \mathbb{Z}/p$ is surjective there exists $u \in K$ such that $\mathrm{tr}_L(u) = 1$. Suppose that $\mathrm{tr}_L(z) = 0$. Then it is straightforwardly verified that the following element β satisfies $\beta^p - \beta = z$:

$$\beta = -\sum_{0 \le i \le n-1} (z + \cdots + z^{p^i}) u^{p^i}$$

where $n = [L : \mathbb{Z}/p]$. – The converse is trivial.

□

In view of Proposition 9 it appears natural to consider the function field

$$E = K(x, y)\,, \qquad y^p - y = f(x)\,. \tag{24}$$

This is called an Artin-Schreier extension of $F = K(x)$. For the following facts we refer to [S], p.115 ff. and p.200 ff. where Artin-Schreier extensions are discussed.

Since $f(x)$ is of degree $d \not\equiv 0 \bmod p$, the field E is a proper extension of F, of degree

$$[E : F] = p\,,$$

and K is the field of constants of E. Moreover $E|F$ is a Galois extension, the automorphisms being given by the substitutions $y \mapsto y + j$ with $j \in \mathbb{Z}/p$.

We are considering the prime divisors, or places, of E; they are denoted by Q. Each such Q induces a prime divisor P in F; we write $Q|P$ to express this situation and say that Q *lies over* P, or that Q *extends* P. According to [S] p.115 ff. there are three types of extensions of places in $E|F$, namely the following.

(1.) *Ramification.* If P ramifies in E then there is only one prime Q of E lying over P, and its ramification degree over P equals p. The residue field is $E_Q = F_P$, i.e., $\deg Q = \deg P$.

The prime $P = P_\infty$, being the only pole of $f(x)$, is the only prime of F which ramifies in E.

We write Q_∞ for the unique extension of P_∞ in E.

(2.) *Splitting.* If P splits in E then there are precisely p primes $Q_1, \ldots, Q_p$ of E which are lying over P. Each of these primes is unramified over P, and the residue field is $E_{Q_i} = F_P$, hence $\deg Q_i = \deg P$ $(1 \le i \le p)$. Let $h_P(x)$ be the characteristic function of P and $\alpha \in F_P$ a root of $h_P(x)$. Splitting occurs precisely for those primes $P \neq P_\infty$ for which there exists $\beta \in F_P$ such that $\beta^p - \beta = f(\alpha)$.

Hence, Proposition 9 *shows that splitting occurs precisely at those primes P of F for which $\chi_f(P) = 1$.*

(3.) *Inertia.* If P is inert in E then there is only one prime Q of E which lies above P and this is unramified. The residue degree is $[E_Q : F_P] = p$, and hence $\deg Q = p \cdot \deg(P)$. Inertia occurs precisely for those primes $P \neq P_\infty$ for which the equation $y^p - y = f(\alpha)$ does not have a root in F_P.

Hence, Proposition 9 *shows that inertia occurs precisely at those primes P of F for which $\chi_f(P) \neq 1$. In this case $\chi_f(P)$ is a primitive p-th root of unity.*

These facts will allow us to connect our L-series with the zeta function of the field E. Before stating the corresponding theorem let us point out that the L-series can be defined not only as an additive series as in (11) but also as a product:

$$L(t \,|\, \chi_f) = \prod_{P \neq P_\infty} \frac{1}{1 - \chi_f(P) t^{\deg P}} = \sum_{\substack{D \ge 0 \\ D \in \mathfrak{D}_f}} \chi_f(D) t^{\deg D}\,, \tag{25}$$

The fact that product and sum coincide follows from: (i) that every positive divisor $D \in \mathfrak{D}_f$ is uniquely representable as a sum of primes $\neq P_\infty$:

$$D = P_1 + \cdots + P_r$$

and (ii) that χ_f is a multiplicative character:

$$\chi_f(D) = \chi_f(P_1) \cdots \chi_f(P_r)\,.$$

Formally, we can include the prime P_∞ in the product and in the sum in (25) by putting $\chi_f(P_\infty) = 0$.

All what we have said about the L-series $L(t\,|\,\chi_f)$ belonging to the canonical character χ of K, remains valid *mutatis mutandis* if we replace χ by a non-trivial power χ^j $(1 \leq j \leq p-1)$. For, χ^j is obtained from χ by an automorphism of the field of p-th roots of unity over $\mathbb{Q}$. In particular we see that $L(t\,|\,\chi_f^j)$ is a polynomial in t of degree $\leq d-1$.

Now we introduce the zeta function [6])

$$Z_E(t) = \prod_Q \frac{1}{1-t^{\deg Q}} = \sum_{N \geq 0} t^{\deg N}$$

where Q ranges over all primes of E (including Q_∞), and N ranges over all positive divisors of E (including those whose support contains Q_∞). The symbol t denotes a complex variable. Again, the fact that product and sum coincide is due to the fact that each positive divisor N is uniquely representable as a sum of prime divisors Q.

Besides $Z_E(t)$ we have to consider the zeta function of the rational field $F = K(x)$, defined as

$$Z_F(t) = \prod_P \frac{1}{1-t^{\deg P}} = \sum_{D \geq 0} t^{\deg D}$$

where P ranges over all primes of F (this time including P_∞) and D over all positive divisors of F (including those which contain P_∞ in their support). For any given $n > 0$ there are $\dfrac{q^{n+1}-1}{q-1}$ positive divisors of degree n. This yields

$$Z_F(t) = \sum_{n \geq 0} \frac{q^{n+1}-1}{q-1} \cdot t^n = \frac{1}{(1-t)(1-qt)}\,.$$

This being said, we now can state:

Theorem 10 *The zeta function $Z_E(t)$ satisfies*

$$Z_E(t) \;=\; Z_F(t) \prod_{1 \leq j \leq p-1} L(t\,|\,\chi_f^j) \;=\; \frac{\displaystyle\prod_{1 \leq j \leq p-1} L(t\,|\,\chi_f^j)}{(1-t)(1-qt)}$$

Proof:

---

[6]) For the general theory of the zeta functions of function fields we refer to [S] pp.158ff.

We work with the product representations of the functions involved. For each prime P of F we show that the product of the terms belonging to P, on the left hand side and on the right hand side, are equal. That is:

$$\prod_{Q|P}(1-t^{\deg Q}) = (1-t^{\deg P}) \prod_{1\le j\le p-1}(1-\chi_f^j(P)t^{\deg P})\,. \tag{26}$$

We distinguish the three types:

(1.) *Ramification.* In this case $P = P_\infty$, $Q = Q_\infty$, $\deg Q_\infty = \deg P_\infty = 1$ and $\chi_f(P_\infty) = 0$. Thus on both sides of (26) we have $1 - t$.

(2.) *Splitting.* Let us put $t^{\deg P} = T$. There are p primes $Q_i|P$, and $\deg Q_i = \deg P$ for each of them. Thus the left hand side of (26) is

$$(1-T)^p\,.$$

In the split case we have $\chi_f(P) = 1$ and therefore also $\chi_f^j(P) = 1$ for $1 \le j \le p-1$. Hence on the right hand side of (26) we have again

$$(1-T)\prod_{1\le j\le p-1}(1-T) = (1-T)^p\,.$$

(3.) *Inertia.* Again let $t^{\deg P} = T$. There is only one prime $Q|P$ and $\deg Q = p\deg P$. Thus the left hand side of (26) is

$$1-T^p\,.$$

In the inert case we know that $\chi_f(P) = \xi \ne 1$, and ξ is a primitive p-th root of unity. Hence on the right hand side of (26) we have again

$$(1-T)\prod_{1\le j\le p-1}(1-\xi^j T) = 1-T^p\,.$$

□

At this point we invoke the general theory of the zeta function of a function field. See [S] p.166 for the following

Theorem 11 *The zeta function $Z_E(t)$ is of the form*

$$Z_E(t) = \frac{L_E(t)}{(1-t)(1-qt)}$$

where $L_E(t) \in \mathbb{Z}[t]$ is a polynomial with integer coefficients, of degree $2g$. Here, g denotes the genus of the function field E.

Since E is an Artin-Schreier extension of F of the form (24), its genus g is computed to be

$$g = \frac{(p-1)(d-1)}{2}\,;$$

see [S] p.115. (Here we use again the fact that $d \not\equiv 0 \bmod p$.) In particular we see that $2g$, the degree of $L_E(t)$, is given by

$$2g = (p-1)(d-1)\,. \tag{27}$$

Now we compare Theorem 11 with Theorem 10 and obtain

$$L_E(t) = \prod_{1 \le j \le p-1} L(t \,|\, \chi_f^j)\,. \tag{28}$$

As said above, the left hand side is a polynomial of degree $(p-1)(d-1)$. Each factor on the right hand side is a polynomial of degree $\le d-1$ by Proposition 8. Comparing degrees, we conclude that each $L(t \,|\, \chi_f^j)$ is of exact degree $d-1$, as claimed in Theorem 2.

In order to deduce Theorem 3 we use the Hasse-Weil Theorem; see [S] p.169:

Theorem 12 *Each root $\rho_1, \ldots, \rho_{2g}$ of $L_E(t)$ has absolute value*

$$|\rho_i| = \sqrt{q^{-1}} \qquad\qquad (1 \le i \le 2g)\,.$$

In view of (28) the roots of $L(t \,|\, \chi_f)$ are among the $2g$ roots of $L_E(t)$ and so we obtain Theorem 3.

6 Generalization to rational functions

In many applications, it is of importance to deal also with exponential sums where $f(x)$ is a non-constant *rational function*, rather than a polynomial. For instance, in the case of

$$f(x) = x + \frac{1}{x}$$

the corresponding exponential sum is known under the name of "Kloosterman sum". Let us discuss the changes which are necessary in the above treatment if we wish to include rational functions too. These changes are mostly straightforward and of a technical nature; the main ideas are the same as for polynomials.

(6.1) Statement of main theorem

If $f(x)$ is a rational function then in the definition (2) of the exponential sum S_f the summation has to be restricted to those elements a for which $f(a)$ is defined, which is to say that a is not a pole of $f(x)$. On the other hand, $a = \infty$ is permitted if ∞ is not a pole of $f(x)$, i.e., if $\deg(f) \leq 0$. Accordingly we write

$$S_f = {\sum_{a \in K \cup \infty}}' \chi\, f(a)\,. \tag{29}$$

where the prime indicates the range of a as explained above. Of course it may happen that $f(a)$ is not defined for any $a \in K \cup \infty$. In this case the above sum is empty and $S_f = 0$. It is easily seen that this does not occur if the order q of K is sufficiently large.

In the case when $f(x)$ is a polynomial, Theorem 1 was formulated under the hypothesis that the degree of f is not divisible by p. If $f(x)$ is a rational function then this hypothesis is to be formulated as follows: *Every pole order of f should not be divisble by p.*

Let $\mathfrak{P}_f$ denote the set of prime divisors of $F = K(x)$ which are poles of f. For each $P \in \mathfrak{P}_f$ we put

$$d_P = -v_P(f)\,.$$

$d_P > 0$ is the pole order of f at P. If f is a polynomial then we have only one pole P_∞ and d_{P_∞} is the degree d of $f(x)$ which appears in the estimate of Theorem 1.

Now in our general case Theorem 1 has to be formulated as follows:

Theorem 13 *Let $f(x)$ be a non-constant rational function. Suppose that all the pole orders d_P of $f(x)$ are not divisible by p, and define d by the formula*

$$d + 1 = \sum_{P \in \mathfrak{P}_f} (d_P + 1) \deg P\,. \tag{30}$$

Then the exponential sum (29) *admits the estimate*

$$|S_f| \leq (d-1)\sqrt{q}\,. \tag{31}$$

Remark: It can be shown, similarly as for polynomials, that each rational function $f(x) \in K(x)$ can be written in the form

$$f(x) = f_1(x) + g(x)^p - g(x)$$

where f_1, g are rational functions and the pole orders of f_1 are not divisible by p. Moreover the poles of f_1 (if there are any) are among the poles of f

and and the pole orders of f_1 are not greater than the corresponding pole orders of f. [7]) From this one deduces that $|S_f| \leq |S_{f_1}| + c$ where c denotes the number of poles of f which are not poles of f_1. Consequently, if f_1 is not constant then the estimate (31) for f_1 implies the same estimate for f. Thus again, the only exceptions to (31) are the rational functions of the form

$$f(x) = c + g(x)^p - g(x)\,.$$

(6.2) The divisor character χ_f

This time we define $\mathfrak{D}_f$ to be the group of those divisors of $F = K(x)$ which do not contain any pole $P \in \mathfrak{P}_f$ in their support. Again the character $\chi_f : \mathfrak{D}_f \to W_p$ will be defined as the composite of a certain divisor homomorphism $\partial_f : \mathfrak{D}_f \to K$ with the canonical character $\chi : K \to W_p$.

In order to define $\partial_f(D)$ for $D \in \mathfrak{D}_f$, it suffices to do it when $D = P$ is a prime divisor of $\mathfrak{D}_f$. Let $f(P)$ denote the residue class of f with respect to P [8]); this is an element in the residue field F_P. (Observe that P is not a pole of f and hence $f(P) \neq \infty$.) Recall that $\mathrm{tr}_P : F_P \to K$ denotes the trace map from F_P to K. Then we define

$$\partial_f(P) = \mathrm{tr}_P\, f(P)\,. \tag{32}$$

If $P = P_a$ is a prime divisor of degree 1 belonging to some element $a \in K \cup \infty$ then $\partial_f(P_a) = f(a)$, as in the case of polynomials. For any divisor $D = \sum_i n_i P_i$ in $\mathfrak{D}_f$ we have

$$\partial_f(D) = \sum_i n_i \partial_f(P_i)\,.$$

Based on this definition, the divisor character χ_f and its L-series $L(t\,|\,\chi_f)$ are defined in the same way as in section 2, and formula (12) holds. It remains to discuss how Theorems 2 and 3 are to be proved in the case of a rational function.

(6.3) The conductor of χ_f

We define the positive divisor M to be

$$M = \sum_{P \in \mathfrak{P}_f} (d_P + 1)P\,. \tag{33}$$

---

[7]) In order to prove this, the rational function $f(x)$ is to be decomposed into its "*principal parts*" which correspond to the poles of f. To each principal part one has to apply the same arguments as for polynomials (which are the principal parts at P_∞).

[8]) For this notation see [S] p.6.

It is called the *enlarged pole divisor* of f. (The word "enlarged" indicates that its multiplicities are $d_P + 1$ and not d_P as in the case of the ordinary pole divisor.) This divisor plays the same role as the divisor $(d+1)P_\infty$ in the case of a polynomial. We have by (30)

$$d + 1 = \deg M\,.$$

Two divisors $D, D' \in \mathfrak{D}_f$ are said to belong to the same *ray class modulo* M if, firstly, $D - D' = (h)$ is a principal divisor of some element $h \in F$ such that, secondly,

$$h \equiv 1 \bmod (d_P + 1)P \qquad\qquad (\text{for each } P \in \mathfrak{P}_f)\,.$$

These simultaneous congruences, for each $P \in \mathfrak{P}_f$, are usually abbreviated in the form

$$h \equiv 1 \bmod M\,. \tag{34}$$

If this is the case then we write

$$D \sim D' \bmod M\,.$$

The next step is to verify the analogue of formula (18) in Lemma 4, i.e., that $\partial_f(D)$ can also be computed by residues of differentials.

At this point, perhaps some words should be said about the notion of "*residue of a differential at* P" in the case when P is a prime divisor of degree > 1. In [S] the residue of a differential is defined for primes of degree 1 only: in that case, one has to choose a prime element u for P and expand the differential in question, say ω, into a Laurent series with respect to this prime element:

$$\omega = \sum_{-\infty \ll \nu} c_\nu u^\nu \mathrm{d}u\,. \tag{35}$$

The coefficients c_ν are contained in K; the symbol $-\infty \ll \nu$ as a summation condition should indicate that the summation starts from some index ν_0 (which may be negative). In this setting, the residue of ω at P is defined to be the coefficient c_{-1}. It is proved that this does not depend on the choice of the prime element u.

Now, if $\deg P = n > 1$ then the expansion (35) into Laurent series with respect to a prime element u is still possible – but this time the coefficients of such expansions are contained in the residue field F_P, not necessarily in K. More precisely: The completion $\widehat{F}_P$ of F with respect to the P-adic

valuation is K-isomorphic to the field of formal power series in u over the residue field F_P. [9]) It is customary to define the residue of ω at P as

$$\mathrm{res}_P(\omega) = \mathrm{tr}_P(c_{-1}) \tag{36}$$

where, as above, $\mathrm{tr}_P : F_P \to K$ denotes the trace function. In the following formulas the residue res_P of a differential is to be understood in this way. If $\deg P = 1$ then the trace tr_P is the identity map and hence we obtain the former definition described above.

We have:

Lemma 14 *Let $D \in \mathfrak{D}_f$ be a divisor of degree 0. Then $D = (h)$ is a principal divisor of some function $h \in F$ and we have*

$$\partial_f(D) = -\sum_{P \in \mathfrak{P}_f} \mathrm{res}_P(f \cdot \mathrm{dlog}\, h) \tag{37}$$

Proof:

(i) Since we work in a rational function field $F = K(x)$, every divisor of degree 0 is a principal divisor.

(ii) First we consider a prime $P \notin \mathfrak{P}_f$; let n_P denote the multiplicity of P in D. Choose a prime element u at P. Since $D = (h)$ we have $v_P(h) = n_P$ and hence

$$h = u^{n_P} z$$

where z is a unit at P, i.e., $v_P(z) = 0$. [10]) Thus

$$\begin{aligned} \mathrm{dlog}\, h &= n_P \cdot \mathrm{dlog}\, u + \mathrm{dlog}\, z \\ \mathrm{res}_P(f \cdot \mathrm{dlog}\, h) &= n_P \mathrm{res}_P(f \cdot \mathrm{dlog}\, u) + \mathrm{res}_P(f \cdot \mathrm{dlog}\, z)\,. \end{aligned}$$

Since P is not a pole of f the P-adic expansion of f is of the form

$$f = c_0 + c_1 u + c_2 u^2 + \cdots$$

with coefficients $c_\nu \in F_P$ and $c_0 = f(P)$. We compute

$$f \cdot \mathrm{dlog}\, u = c_0 \cdot \mathrm{dlog}\, u + \cdots = f(P) \cdot \frac{\mathrm{d}u}{u} + \cdots$$

---

[9]) The standard reference for this is the book *Hasse, Zahlentheorie*, which has also been translated into English. See in particular chapter II of that book.

[10]) The functions u and z depend on the choice of P and, hence, should be denoted by u_P, z_P. But since P is fixed for the moment we prefer the simpler notation u, z.

where the dots $\cdots$ indicate differentials which are holomorphic at P, hence have no residue. The differential

$$f \cdot \mathrm{dlog}\, z = f \cdot \frac{\mathrm{d}z}{z}$$

is also holomorphic at P since z is a unit at P. Using the definition (36) we conclude

$$\mathrm{res}_P(f \cdot \mathrm{dlog}\, h) = n_P \cdot \mathrm{res}_P(f(P)\frac{\mathrm{d}u}{u}) = n_P \cdot \mathrm{tr}_P\, f(P) = n_P \cdot \partial_f(P)\,,$$

according to (32). Since $D = \sum_{P \notin \mathfrak{P}_f} n_P P$ we see that

$$\sum_{P \notin \mathfrak{P}_f} \mathrm{res}_P(f \cdot \mathrm{dlog}\, h) = \partial_f(D).$$

(iii) Now we apply the well known *residue theorem* for differentials, which says that the sum of all residues of a differential is zero:

$$\sum_{P \notin \mathfrak{P}_f} \mathrm{res}_P(f \cdot \mathrm{dlog}\, h) + \sum_{P \in \mathfrak{P}_f} \mathrm{res}_P(f \cdot \mathrm{dlog}\, h) = 0\,,$$

We obtain (37).

□

Remark: When we compare Lemma 14 with Lemma 4 then we observe that Lemma 4 is formulated in more generality, namely for a divisor D of arbitrary degree, not necessary of degree 0. The reason for this is that in our more general situation here it is not always true that there exists $h \in F$ with $D = (h)_f$, i.e., such that the principal divisor of h represents D except at the poles of f. It is easily verified that such h exists if and only if the degree $\deg D$ is a multiple of the greatest common divisor of the degrees $\deg P$ for $P \in \mathfrak{P}_f$. If this condition is satisfied then the relation $D = (h)_f$ implies the validity of formula (37): in fact we can use exactly the same proof as above. – In the following we shall use (37) in the case of divisors of degree 0 only.

Now, the analogue of Proposition 5 in our more general situation reads as follows:

Proposition 15 *If $D \sim 0 \bmod M$ then $\partial_f(D) = 0$. Hence the homomorphism $\partial_f : \mathfrak{D}_f \to K$ depends only on the ray classes of $\mathfrak{D}_f$ modulo M. Moreover, when all the pole orders of f are not divisible by p then M is the smallest modulus with this property. More precisely: If M' is another divisor such that $0 \leq M' < M$ then ∂_f induces a surjection from the group of divisors $D \sim 0 \bmod M'$ onto K.*

Proof:

(i) Suppose that $D \sim 0 \bmod M$. Then $D = (h)$ with $h \equiv 1 \bmod M$. Let $P \in \mathfrak{P}_f$. We choose a prime element u for P. Since $h \equiv 1 \bmod (d_P+1)P$, we see that its P-adic expansion is of the form

$$h = 1 + au^{d_P+1} + \cdots$$

with $a \in F_P$, where the dots indicate terms of higher order. We differentiate:

$$\mathrm{d}h = (d_P+1)au^{d_P}\mathrm{d}u + \cdots$$

and multiply with $h^{-1} \equiv 1 \bmod (d_P+1)P$:

$$\mathrm{dlog}\, h = (d_P+1)au^{d_P}\mathrm{d}u + \cdots .$$

Here, the dots indicate terms of order $\geq d_P+1$. We see that $v_P(\mathrm{dlog}\, h) \geq d_P$ (and $= d_P$ if $(d_P+1)a \neq 0$). On the other hand, the function f has a pole at P of order d_P, which is to say that $v_P(f) = -d_P$. We conclude that

$$v_P(f \cdot \mathrm{dlog}\, h) \geq 0\,,$$

i.e., the differential $f \cdot \mathrm{dlog}\, h$ is holomorphic at P and hence has no residue.

This holds for every $P \in \mathfrak{P}_f$. From (37) we infer that $\partial_f(D) = 0$.

(ii) Now let $0 \leq M' < M$ be a smaller modulus. There exists at least one prime divisor $P \in \mathfrak{P}_f$ whose multiplicity in M' is strictly smaller than its multiplicity in D (which is d_P+1). Hence we have $M' \leq M - P$, and it suffices to prove the assertion of Proposition 15 for $M-P$ instead of M'. We have

$$M - P = d_P P + \sum_{\substack{Q \in \mathfrak{P}_f \\ Q \neq P}} (d_Q+1)Q\,.$$

Let $D \in \mathfrak{D}_f$ be such that $D \sim 0 \bmod M-P$. Then $D = (h)$ with $h \equiv 1 \bmod M-P$. If $Q \in \mathfrak{P}_f$, $Q \neq P$ then $h \equiv 1 \bmod (d_Q+1)Q$, and the same argument as in (i) shows that $\mathrm{res}_Q(f \cdot \mathrm{dlog}\, h) = 0$. Therefore, in order to compute $\partial_f(D)$ we only have to compute the residue $\mathrm{res}_P(f \cdot \mathrm{dlog}\, h)$ at the one single prime divisor P.

We have $h \equiv 1 \bmod d_P P$, and hence the P-adic expansion of h is of the form

$$h = 1 + bu^{d_P} + \cdots \tag{38}$$

with $b \in F_P$. From this we deduce similarly as above that

$$\mathrm{dlog}\, h = d_P b u^{d_P-1}\mathrm{d}u + \cdots = d_P b u^{d_P}\frac{\mathrm{d}u}{u} + \cdots .$$

The function f has a pole of order d_P and so its expansion at P is of the form

$$f = cu^{-d_P} + \cdots$$

with $c \neq 0$. Thus

$$\begin{aligned} f \cdot \mathrm{dlog}\, h &= d_P bc \cdot \frac{\mathrm{d}u}{u} + \cdots \\ \mathrm{res}_P(f \cdot \mathrm{dlog}\, h) &= d_P \cdot \mathrm{tr}_P(bc) \\ \partial_f(D) &= -d_P \cdot \mathrm{tr}_P(bc)\,. \end{aligned}$$

The trace map $\mathrm{tr}_P : F_P \to K$ is surjective. If the pole order $d_P \not\equiv 0 \bmod p$ we conclude that the map $b \mapsto -d_P \cdot \mathrm{tr}_P(bc)$ is also surjective to K. (Note that have $c \neq 0$ as said above already.)

It remains to verify that to every $b \in F_P$ there exists a divisor $D \in \mathfrak{D}_f$ of degree 0 such that, firstly, $D \sim 0 \bmod M - P$, and secondly this given b appears in the expansion (38).

Indeed, this is an immediate consequence of the so-called *weak approximation theorem* for valuations. [11]) Accordingly, given $b \in F_P$ and a prime element u for P there exists $h \in F$ such that

$$\begin{aligned} h &\equiv 1 + bu^{d_P} \mod (d_P + 1)P \\ h &\equiv 1 \mod (d_Q + 1)Q \qquad \text{if } Q \in \mathfrak{P}_f,\ Q \neq P\,. \end{aligned}$$

Then the principal divisor $D = (h)$ satisfies our requirements.

□

From Proposition 15 we obtain the following result for χ_f, which is the generalization of Proposition 6 in section 3 and is obtained in the same way as there.

Proposition 16 *As above, M denotes the extended pole divisor of $f(x)$. The character $\chi_f : \mathfrak{D}_f \to W_p$ is a ray character modulo M, which means that $\chi_f(D)$ depends only on the ray class of D modulo M. Moreover, if all pole orders of f are $d_P \not\equiv 0 \bmod p$ then M is the smallest modulus with this property, in fact: for $0 \leq M' < M$ the map χ_f induces a surjection from the group of divisors $D \sim 0 \bmod M'$ onto W_p.*

Accordingly M is then called the *conductor* of the divisor character χ_f.

(6.4) The L-series as a polynomial

In the general case of a rational function $f(x)$ we have to reformulate Lemma 7 as follows.

---

[11]) See [S] page 11.

Lemma 17 *For each $n \in \mathbb{Z}$ there exists a divisor $D \in \mathfrak{D}_f$ of degree n. The number of ray classes modulo M of degree n is finite and it does not depend on n. If $n \geq d$ then every ray class modulo M of degree n contains a positive divisor, and the number of positive divisors in each such ray class is q^{n-d}.*

Proof:

(i) For every integer $n > 0$ there exist irreducible polynomials in $K[x]$ of degree n. (This is so because there exists a field extension of K of degree n.) We choose one such irreducible polynomial and let P_n be the corresponding prime divisor of $F = K(x)$. If n is different from the finitely many degrees $\deg P$ for $P \in \mathfrak{P}_f$ then $P_n \notin \mathfrak{P}_f$ and hence P_n is contained in $\mathfrak{D}_f$. Otherwise, we choose two auxiliary integers $n_1, n_2 > 0$ which are different from the finitely many degrees $\deg P$ for $P \in \mathfrak{P}_f$, and such that they are relatively prime to each other. Then every integer $n \in \mathbb{Z}$ can be written in the form $n = \lambda_1 n_1 + \lambda_2 n_2$ with $\lambda_1, \lambda_2 \in \mathbb{Z}$. The divisor $D = \lambda_1 P_{n_1} + \lambda_2 P_{m_2}$ is contained in $\mathfrak{D}_f$ and is of degree n.

(ii) Let $n \in \mathbb{Z}$. We fix a divisor $A \in \mathfrak{D}_f$ of degree n. Let D range over all divisors of degree n in $\mathfrak{D}_f$. Then the map $D \mapsto D - A$ establishes a $1-1$ correspondence between the ray classes modulo M of degree n and the ray classes modulo M of degree 0. Hence the number of ray classes of given degree n equals the number of ray classes of degree 0.

Now let $n = 0$. If $D \in \mathfrak{D}_f$ is of degree 0 then $D = (h)$ is a principal divisor. h has no pole or zero in $\mathfrak{P}_f$. We denote by $\mathcal{O}_{\mathfrak{P}_f}$ the ring of all functions which have no pole in $\mathfrak{P}_f$. Hence h is a unit in this ring.

By definition of ray classes, the congruence class of h modulo M determines the ray class of D modulo M. From this we infer that there are only finitely many ray classes of degree 0, because there are only finitely many congruence classes in $\mathcal{O}_{\mathfrak{P}_f}$ modulo M. In fact, the following arguments show that there are precisely q^{d+1} such congruence classes:

(iii) For each $P \in \mathfrak{P}_f$ we choose a prime element u_P for P. Every function $h \in \mathcal{O}_{\mathfrak{P}_f}$ admits a P-adic expansion of the form

$$h = c_{P,0} + c_{P,1} u_P + c_{P,2} u_P^2 + \cdots \qquad (\text{at } P) \tag{39}$$

with coefficients $c_{P,\nu} \in F_P$. If we deal with congruences in $\mathcal{O}_{\mathfrak{P}_f}$ modulo M then, by definition (34), this means simultaneous congruences modulo $(d_P + 1)P$ for all $P \in \mathfrak{P}_f$. This in turn means that only the first $d_P + 1$ coefficients $c_{P,0}, c_{P.1}, \ldots, c_{P,d_P}$ in the expansion (39) are relevant. In other words:

Two functions $h, h' \in \mathcal{O}_{\mathfrak{P}_f}$ are congruent modulo M if and only if for each $P \in \mathfrak{P}_f$, the first $d_P + 1$ coefficients of their expansions coincide: $c_{P,\nu} = c'_{P,\nu}$ for $0 \le \nu \le d_P$.

Again from the "*weak approximation theorem*" we infer: given for each $P \in \mathfrak{P}_f$ arbitrary coefficients $c_{P,\nu}$ $(0 \le \nu \le d_P)$ then there exists $h \in \mathcal{O}_{\mathfrak{P}_f}$ such that

$$h \equiv c_{P,0} + c_{P,1} u_P + \cdots + c_{P,\nu} u_P^{d_P} \bmod (d_P + 1)P \qquad (P \in \mathfrak{P}_f)\,.$$

In other words: the residue classe in $\mathcal{O}_{\mathfrak{P}_f}$ modulo M are uniquely described by the vectors of coefficients $(c_{P,0}, \ldots, c_{P,d_P})$ which may range freely over F_P (for $P \in \mathfrak{P}_f$). Since F_P has $q^{\deg P}$ elements we conclude: there are precisely

$$\prod_{P \in \mathfrak{P}_f} q^{\deg P (d_P + 1)} = q^{d+1}$$

residue classes in $\mathcal{O}_{\mathfrak{P}_f}$ modulo M. (Recall the definition (30) of the integer d.)

(iv) Now suppose that $n \ge d$, and let $A \in \mathfrak{D}_f$ be a fixed divisor of degree n. We are going to show that there exists a positive divisor $D \ge 0$ of degree n in $\mathfrak{D}_f$ such that $D \sim A \bmod M$. This means that $D - A = (h)$ should be the principal divisor of an element $h \equiv 1 \bmod M$.

Let $\mathcal{L}(A)$ denote the K-vector space consisting of those functions $h \in F$ for which $(h) \ge -A$ (together with 0). [12]) This means $(h) = D - A$ with $D \ge 0$. We have to show that among these functions $h \in \mathcal{L}(A)$ there is at least one for which $h \equiv 1 \bmod M$.

For any function $0 \ne h \in \mathcal{L}(A)$, the poles of h are among the prime divisors appearing in A, hence are not in $\mathfrak{P}_f$. Thus $h \in \mathcal{O}_{\mathfrak{P}_f}$. If we deal with congruence classes modulo M then we work in the factor ring $\mathcal{O}_{\mathfrak{P}_f}/M$. Consider the map

$$\varrho : \mathcal{L}(A) \to \mathcal{O}_{\mathfrak{P}_f}/M$$

which is obtained by mapping each $h \in \mathcal{L}(A)$ onto its congruence class modulo M. We have to show that among the functions $h \in \mathcal{L}(A)$ there is one for which $\varrho(h) = 1$. To this end we shall show that ϱ *is surjective*.

We regard ϱ as a K-linear map of vector spaces. The surjectivity of ϱ will follow from the computation of the K-dimensions of the vector spaces in question.

First, since $\deg A = n \ge 0$ we have that

$$\dim \mathcal{L}(A) = 1 + \deg A\,. \tag{40}$$

[12]) For this notation see [S] page 16.

In fact, this is a special case of the *Riemann-Roch theorem* [13]) when we observe that the rational function field $F = K(x)$ has genus $g = 0$. On the other hand, the above formula can also be proved directly, by elementary means, as follows: Consider the infinite prime P_∞ which is of degree 1. The divisor $A - nP_\infty$ is of degree 0, hence a principal divisor: $A - nP_\infty = (z)$ with $z \in F$. Thus $A \sim nP_\infty$ and hence $\dim \mathcal{L}(A) = \dim \mathcal{L}(nP_\infty)$. On the other hand, $\mathcal{L}(nP_\infty)$ is the K-vector space of all polynomials of degree $\leq n$ and therefor $\dim \mathcal{L}(nP_\infty) = 1 + n$. [14])

By the way, the relation (40) for divisors A holds not only if $\deg A \geq 0$ but also if $\deg A = -1$. For, in this case we have $\mathcal{L}(A) = 0$ and so $\dim \mathcal{L}(A) = 0 = 1 + (-1)$. We shall use this remark below.

The kernel of the map ϱ consists of those functions $h \in \mathcal{L}(A)$ for which $h \equiv 0 \bmod M$, which is to say that $(h) \geq M$ (or $h = 0$). On the other hand, we have $(h) \geq -A$. Since A and M have disjoint support, this implies $(h) \geq M - A$, i.e., $h \in \mathcal{L}(A - M)$. *Thus the kernel of ϱ is $\mathcal{L}(A - M)$.*

Using our assumption that $n \geq d$, we see that $\deg(A-M) = n-(d+1) \geq -1$. By what was said above this implies

$$\dim \mathcal{L}(A - M) = 1 + \deg(A - M) = (1 + \deg A) - \deg M \qquad (41)$$

and so

$$\dim \mathcal{L}(A) - \dim \mathcal{L}(A - M) = \deg M = d + 1 .$$

It follows that the image of ϱ is a K-vector space of dimension $d + 1$.

Hence, in order to prove the surjectivity of $\varrho : \mathcal{L}(A) \to \mathcal{O}_{\mathfrak{P}_f}/M$ we have to verify that $\mathcal{O}_{\mathfrak{P}_f}/M$ is also of dimension $d + 1$.

Indeed: we have shown in (iii) above that $\mathcal{O}_{\mathfrak{P}_f}/M$ has precisely q^{d+1} elements, hence $\dim \mathcal{O}_{\mathfrak{P}_f}/M = d + 1$.

(v) We have seen in (iv) that there exists $h \in \mathcal{L}(A)$ such that $h \equiv 1 \bmod M$. Also, we have seen that there exists a $1 - 1$ correspondence between such elements h and the positive divisors $D \geq 0$ in $\mathfrak{D}_f$ with $D \sim A$; this correspondence is given by the relation

$$D - A = (h) .$$

In order to count those positive divisors D we have to count the corresponding elements $h \in \mathcal{L}(A)$.

Let us fix some $h_0 \in \mathcal{L}(A)$ with $h_0 \equiv 1 \bmod M$. Any other such element h has the form $h = h_0 + z$ where $z \equiv 0 \bmod M$, hence $z \in \mathcal{L}(A - M)$. We

[13]) See [S] page 29, Theorem I.5.17.

[14]) See [S] page 22, I.4.18.

have seen in (iv) that $\mathcal{L}(A-M)$ has dimension $(1+n)-(d+1)=n-d$. Hence there are q^{n-d} elements $z \in \mathcal{L}(A-M)$, and they correspond to as many $h \in \mathcal{L}(A)$ with $h \equiv 1 \bmod M$.

□

Remark. It is possible to compute the number of ray classes modulo M of degree 0 explicitly. To this end, we first have to count the number of units h of $\mathcal{O}_{\mathfrak{P}_f}$ modulo M. Secondly we have to divide this number by $q-1$ because if $D=(h)$ then also $D=(c \cdot h)$ for the $q-1$ elements $0 \neq c \in K$. The computation gives the number

$$\frac{1}{q-1} \prod_{P \in \mathfrak{P}_f} (q^{\deg P}-1) q^{d_P \deg P}.$$

We leave the details to the reader.

□

Having established Lemma 17, which is the generalization of Lemma 7, it is now possible to prove Proposition 8 also in the general case of rational functions, with precisely the same proof as in section 4.

(6.5) Artin-Schreier extensions of $K(x)$

As to the Artin-Schreier extension

$$E=K(x,y), \qquad y^p-y=f(x)$$

the only essential difference to the discussion in section 5 is that now, there is not only one ramified prime but every pole $P \in \mathfrak{P}_f$ ramifies in E. Otherwise the same arguments as in the proof of Theorem 10 work also in our general case.

In the course of that discussion it is necessary to verify that the genus g of E now is given by the same formula (27) as stated in section 5. See [S] p.115.

7 References

The following list contains the standard references used in the text, and in addition some recent publications for further reading on the subject.

[S] H. Stichtenoth, *Algebraic function fields and codes.* Universitext Springer (1991)

[H] H. Hasse, *Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper.*
Journ. f.d.r.u.a. Mathematik (Crelle's Journal) **172**, 37–54 (1934)

[H-D] H. Hasse, H. Davenport, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen.*
Journ. f.d.r.u.a. Mathematik (Crelle's Journal) **172**, 151–182 (1934)

[G] V. Gillot, *Bounds for exponential sums over finite fields.*
Finite fields and their applications **1, No. 4** 421–436 (Oct 1995)

[V-V] G. van der Geer, M. van der Vlugt, *How to construct curves over finite fields with many points*.
Algebraic geometry e-prints, alg-geom/9511005 (1995) 21p.

Mathemat. Inst. Univ. Heidelberg
Im Neuenheimer Feld 288
D–69120 Heidelberg, Germany

e-mail: roquette@mathi.uni-heidelberg.de