ACTA ARITHMETICA
LIX.3 (1991)

Multiplicative character sums and Kummer coverings

by

MARC PERRET (Marseille)

0. Introduction. Let $k = \boldsymbol{F}_q$ be the finite field with q elements, χ a character of the multiplicative group k^*, X an absolutely irreducible curve defined over k, f a rational function on X, and $X'(k)$ the set of rational points of X over k, such that $f(x) \neq 0$ and $f(x) \neq \infty$. We are interested in the sum

$$W(k,f) = \sum_{x \in X'(k)} \chi(f(x)).$$

Class field theory and Kummer theory enable us to compute this sum via the theory of abelian L-functions. This is a classical method due to Hasse which uses Artin–Schreier theory in the additive case, developed by Weil, Bombieri, Deligne, Katz, ...

We follow here a recent paper of Lachaud [3], which deals with the additive case.

In Section I, we recall some Kummer theory, and some class field theory in Section II. We compute in Section III the conductor and the genus of a Kummer covering $\pi\colon Y \to X$; this enables us to link in Section IV the character sums $W(k,f)$ with the L-functions of X and Y. From these results we derive in Section V a bound for $\# Y(k) - \# X(k)$ in terms of q and the genus of X and Y, that generalize in this case the well known Weil inequality.

I. Kummer theory.

(1.1) Let p be a prime number, K a field of characteristic p, n a positive integer, and $a \in K$. We suppose that K contains the group $\mu_n(K)$ of nth roots of unity. Let r be the lowest integer such that $a^r \in K^n$. Then the subfield L of a given algebraic closure Ω of K, generated by the roots of the polynomial $X^n - a$, is a cyclic extension of K, with $[L:K] = r$. In particular, $X^n - a$ is irreducible over K if and only if $r = n$ (cf. [1, p. 87]).

If $A \subset K^*$, we denote by $K(A^{1/n})$ the extension of K defined by the elements $x \in \Omega$ such that $x^n \in A$.

Let H be a subgroup of K^* containing K^{*n}. For each $a \in H/K^{*n}$, let $\theta_a \in \Omega$ be such that θ_a^n represents a in H modulo K^{*n}. Then the set

$\{\theta_a;\ a\in H/K^{*n}\}$, forms a basis of the K-vector space $K(H^{1/n})$ (cf. [1, p. 85]). Hence,

$$\mathrm{Gal}(K(H^{1/n})/K)\approx H/K^{*n},$$

and

$$[K(H^{1/n}):K]=(H:K^{*n}).$$

The extension $K(H^{1/n})$ is generated by the roots of the equation $X^n-a=0$, where a runs over a system of representatives of H/K^{*n}.

The correspondence $H\to K(H^{1/n})$ is an increasing one-to-one mapping from the set of subgroups of K^* containing K^{*n} onto the set of abelian subextensions of Ω, whose exponent divides n (cf. [1, p. 85]).

Let G be the Galois group $\mathrm{Gal}(K(H^{1/n})/K)$. If $\sigma\in G$ and $h\in H$, then there exists $x\in K(H^{1/n})$ such that $x^n=h$; we can then define

$$\langle\sigma, h\rangle=\frac{\sigma(x)}{x}\in\mu_n(K).$$

This map induces a nondegenerate bimultiplicative map, also denoted by $\langle\cdot,\cdot\rangle$ (see [4, p. 329]),

$$G\times H/K^{*n}\to\mu_n(K).$$

(1.2) Let X be a smooth irreducible projective curve defined over a finite field k, and let $K=R(X)$ be the field of rational functions of X over k. Then K is an extension of k of transcendence degree 1. We suppose that K/k is a regular extension, i.e. the following equivalent conditions hold, where $\boldsymbol{F}$ is an algebraic closure of k:

(i) $K\otimes_k\boldsymbol{F}$ is a field;
(ii) The exact constant field of K is k;
(iii) K and $\boldsymbol{F}$ are linearly disjoint;
(iv) The curve X is absolutely irreducible.

Moreover, if these conditions hold, then the field $\tilde K=\boldsymbol{F}(X)$ is isomorphic to $K\otimes_k\boldsymbol{F}$.

(1.3) Lemma. *Let H_0 be a subgroup of K^*, containing K^{*n} as a subgroup of finite index. Then the extension $K(H^{1/n})|K$ is regular if and only if $\tilde K^{*n}\cap H_0=K^{*n}$.*

Proof. Let $\tilde H=H_0\tilde K^{*n}$. There is a canonical surjective morphism

$$\varphi\colon K(H_0^{1/n})\otimes_k\boldsymbol{F}\to\tilde K(H_0^{*n}),$$

hence $K(H_0^{1/n})\otimes_k\boldsymbol{F}$ is a field if and only if φ is an isomorphism. But

$$[K(H_0^{1/n})\otimes_k\boldsymbol{F}:\tilde K]=(H_0:K^{*n}),$$
$$[\tilde K(H_0^{1/n}):\tilde K]=(\tilde H:\tilde K^{*n})=(H_0:\tilde K^{*n}\cap H_0).$$

So,

$$K(H_0^{1/n})\otimes_k\boldsymbol{F}\text{ is a field}\Leftrightarrow(H_0:\tilde K^{*n}\cap H_0)=(H_0:K^{*n})\Leftrightarrow\tilde K^{*n}\cap H_0=K^{*n},$$

since we always have $K^{*n}\subset\tilde K^{*n}\cap H_0$. ∎

For convenience, we will say that a subgroup H_0 of K^*, containing K^{*n} as a subgroup of finite index, is *regular* if the corresponding extension $K(H_0^{1/n})/K$ is regular.

(1.4) Let $k=\boldsymbol{F}_q$ be the finite field with q elements, K a function field of one variable over k, and $n\geqslant 2$ an integer such that n divides $q-1$ (then K contains the group of nth roots of unity). If u is a place of K, we denote by v_u the normalized valuation of K defined by u. For $f\in K$, we define the *reduced order* of f at u by

$$v'_u(f)=\min_{g\in K^*}(|v_u(fg^n)|)$$

(where $|x|$ is the absolute value of $x\in\boldsymbol{R}$), therefore

$$v'_u(f)=0\Leftrightarrow f\in\mathcal{O}_u^*\cdot K^{*n},$$

where $\mathcal{O}_u$ is the ring of regular functions at u.

(1.5) Proposition. *Let $f\in K^*$. There exists $h\in K^*$ such that*

$$f\equiv h\pmod{K^{*n}}\quad\textit{and}\quad 0\leqslant v_u(h)<n.$$

Moreover,

$$v'_u(f)=v_u(h).$$

In particular, $0\leqslant v'_u(f)<n$.

Proof. If $f\in K^*$, let π be a local parameter at the place u. Since $v'_u(f)$ is defined by an absolute value, we can suppose that $v=v_u(f)\geqslant 0$. So we can write f as

$$f=\sum_{i=v}^{\infty}a_i\pi^i.$$

If $v\geqslant n$, let $v=an+r$ with $0\leqslant r<n$ be the division of v by n, and define $g=\pi^{-a}$; then

$$fg^n=a_v\pi^r+\sum_{i>r}b_i\pi^i\quad\text{and}\quad v_u(fg^n)=r,$$

which shows that

$$0\leqslant v'_u(f)\leqslant v_u(fg^n)=r<n.$$

It is clear that under the assumptions of the proposition, we have $v'_u(f)\leqslant v_u(h)$. If there exists $h'\equiv f\pmod{K^{*n}}$, with $v_u(h')\leqslant v_u(h)$, then, writing

$h' = fg'^n$, we have

$$0 \leqslant v_u(fg'^n) \leqslant v_u(fg^n) < n, \qquad v_u(fg'^n) - v_u(fg^n) = n v_u(g'/g) \in n\mathbf{Z},$$

hence the equality

$$v'_u(f) = v_u(h') = v_u(h). \ \blacksquare$$

II. Class field theory.

(2.1) Local theory. We recall here some results we need for our purposes that we extract from [5], particularly p. 212, 215, and [2]. Let K be a local field, and L/K a finite extension of degree $n \geqslant 2$ dividing $q-1$, hence K contains the group $\mu_n(K)$ of nth roots of unity. We denote by u a discrete valuation of K for which K is complete.

If $\chi \in \mathrm{Hom}(G, \frac{1}{n}\mathbf{Z}/\mathbf{Z})$, and if $b \in K^*$, we can define, using the cup-product, an element $(\chi, b) \in \mathrm{Br}(L/K)$, the Brauer group of L/K. Moreover, there is a canonical isomorphism

$$\mathrm{Inv}_K\colon\ \mathrm{Br}(L/K) \to \tfrac{1}{n}\mathbf{Z}/\mathbf{Z},$$

so we can define

$$(\chi, b)_u = \mathrm{Inv}_K(\chi, b) \in \tfrac{1}{n}\mathbf{Z}/\mathbf{Z}.$$

Let ω be a primitive element of $\mu_n(K)$. For $a \in K^*$, there is a unique character $\chi_a \in \mathrm{Hom}(G, \frac{1}{n}\mathbf{Z}/\mathbf{Z})$ such that

$$(a, b) = (\chi_a, b) \in \mathrm{Br}(L/K) \tag{2.1.1}$$

and

$$(a, b)_u = \omega^{n\cdot \mathrm{Inv}_K(a,b)} = \omega^{n\cdot \mathrm{Inv}_K(\chi_a, b)} \in \mu_n(k) = \mu_n(K), \tag{2.1.2}$$

for $a, b \in K^*$.

Then we have

$$(a, b)_u = \left((-1)^{\alpha\beta}\,\overline{a^{\beta}\cdot b^{-\alpha}}\right)^{(q-1)/n} \tag{2.1.3}$$

with $\alpha = u(a)$, $\beta = u(b)$, and where $\bar{x}$ denotes the image of $x \in K$ in k.

(2.2) Global theory. Let K be a function field of one variable over k, and L/K an extension of degree $n \geqslant 2$. We assume that K contains the group $\mu_n(K)$ of nth roots of unity. Let I_K denote the idele group of K, and G the Galois group $\mathrm{Gal}(L/K)$. For a place u of K and a place w of L dividing u, we denote by G_u the Galois group $\mathrm{Gal}(L_w/K_u)$, by j_u the canonical injection $K_u^* \to I_K$, and by ϱ_u the injection $G_u \to G$.

For $a, b \in K_u^*$, we define a symbol $(a, b)_u$ by formula (2.1.2); according to (2.1.3) this symbol satisfies

$$(a, b)_u = N_{k(u)/k}\left((-1)^{\alpha\beta}\,\overline{a^{\beta}\cdot b^{-\alpha}}\right)^{(q-1)/n} \in \mu_n(k),$$

where α and β are as defined before.

Let $\mathscr{A}$ be the Artin reciprocity map; then the sequence

$$1 \to K^* N_{L/K}(I_L) \to I_K \xrightarrow{\mathscr{A}} G \to 1$$

is exact (see [2]).

If $f \in K^*$, let $\alpha \in \Omega$ be a solution of the equation $\alpha^n = f$. We have defined the symbol

$$\langle \sigma, f\rangle = \frac{\sigma(\alpha)}{\alpha} \in \mu_n(K) \qquad \text{for } \sigma \in G.$$

(2.2.1) Lemma. *Let $f \in K^*$, and $z \in I_K$. Then*

$$(f, z_u)_u = (\chi_{f,u}, z_u)_u \in \mu_n(K), \qquad \langle \mathscr{A}(z), f\rangle = \prod_u (f, z_u)_u.$$

Proof. For every character $\chi_0 \in \mathrm{Hom}(G, \mathbf{Q}/\mathbf{Z})$, and for every idele $z \in I_K$,

$$\chi_0 \circ \mathscr{A}(z) = \sum_u \mathrm{Inv}_{K_u}(\chi_0 \circ \varrho_u, z_u) \in \tfrac{1}{n}\mathbf{Z}/\mathbf{Z}$$

([2, p. 189]). Hence, if ω is a primitive n-root of unity in k,

$$\omega^{\chi_0 \circ \mathscr{A}(z)} = \prod_u \omega^{n\cdot \mathrm{Inv}_{K_u}(\chi_0 \circ \varrho_u, z_u)}. \tag{2.2.2}$$

If $\chi_{0,f} \in \mathrm{Hom}(G, \mathbf{Q}/\mathbf{Z})$ is the character associated to f, then ([5, p. 213])

$$\langle \sigma, f\rangle = \omega^{n\cdot \chi_{0,f}(\sigma)}.$$

Lemma (2.2.1) is then a reformulation of (2.1.1) and (2.1.2), using (2.2.2). $\blacksquare$

III. The genus of a Kummer covering.

We make the same assumptions as in (2.2). Let $\chi \in \hat{k}^*$ be a character of the multiplicative group of $k = \mathbf{F}_q$, and let u be a place of K. In all this paper, we shall assume that the following assumptions hold:

(†) $\mathrm{Ker}\,\chi \cap \mu_n(k) = \{1\}$ and $\chi^{(q-1)/n} \circ N_{k(u)/k} \neq 1$ for every place u of K.

Such a character always exists, we can choose for example a generator χ of the cyclic group $\hat{k}^*$.

The symbol $(a, b)_u$ defines a bimultiplicative map from $K_u^* \times K_u^*$ into $\mu_n(k)$, with kernel K_u^{*n} on the left and on the right (see [4, p. 215]). Hence, it defines a nondegenerate bimultiplicative map

$$K_u^*/K_u^{*n} \times K_u^*/K_u^{*n} \to \mu_n(k).$$

For $a, b \in K_u^{*n}$, define

$$\{a, b\}_u = \chi((a, b)_u).$$

In order to extend this to a character of I_K, we put, for $z \in I_K$ and $f \in K^*$,

$$\omega_f(z) = \prod_u \{f, z_u\}_u.$$

Note that ω_f depends on χ.

(3.1) Proposition. *Suppose that χ satisfies conditions (†), and let $U'(f)$ be the set of places u of K such that $v'_u(f) > 0$. Then the ramification set $R(\omega_f)$ of ω_f is equal to $U'(f)$, and its conductor is given by*

$$\mathfrak{f}(\omega_f) = \sum_{u \in U'(f)} u.$$

Proof. If u is a place of K, let $\mathcal{O}_u$ be the ring of regular functions at u, and $\mathfrak{p}_u$ its maximal ideal. We write $\omega_u(z)$ instead of $\{f, z\}_u$, for every $z \in K_u^*$. By definition of the conductor, $\mathfrak{f}(\omega_f) = \sum_u \mathfrak{f}_u u$, where $\mathfrak{f}_u$ is the smallest integer $k \geqslant 0$ such that $\omega_u(z) = 1$ for every $z \in 1 + \mathfrak{p}_u^k$.

Let $f \equiv h \pmod{K^{*n}}$, with $h \in \mathcal{O}_u^*$, such that $v'_u(f) = v_u(h) = v$. Then $f = g^n \cdot h$, $g \in K^*$ and, if $z \in \mathcal{O}_u^*$,

$$(f, z)_u = (h, z)_u = N_{k(u)/k}\big((-1)^{\alpha\beta}\overline{h^\beta \cdot z^{-\alpha}}\big)^{(q-1)/n},$$

with $\alpha = v_u(h) = v$ and $\beta = v_u(z) = 0$. Hence,

$$(f, z)_u = N_{k(u)/k}(\bar{z})^{-v(q-1)/n}.$$

There are two cases:

- If $u \notin U'(f)$, then $v = 0$, and $(f, z)_u = 0$, so $\mathfrak{f}_u = 0$.
- If $u \in U'(f)$, since $\chi^{(q-1)/n} \circ N_{k(u)/k} \neq 1$, we have $\mathfrak{f}_u \geqslant 1$. On the other hand, if $z \in 1 + \mathfrak{p}_u$, then $\bar{z} = 1$, so $(f, z)_u = 0$, and $\mathfrak{f}_u = 1$, which proves the proposition. ■

Let H be a subgroup of K^*, containing K^{*n} as a subgroup of finite index. Kummer theory gives (see (1.1)) a nondegenerate bimultiplicative morphism

$$G \times H/K^{*n} \to \mu_n(k)$$
$$(\sigma, \bar{h}) \mapsto \langle \sigma, h \rangle.$$

For $f \in K^*$, we consider the character $\chi_f \in \hat{G} = \operatorname{Hom}(G, \boldsymbol{C}^*)$ associated to f by class field theory (cf. § II)

$$\chi_f \colon G \to \boldsymbol{C}^*$$
$$\sigma \mapsto \chi(\langle \sigma, f \rangle).$$

This defines a morphism

$$\theta \colon H/K^{*n} \to \hat{G}$$
$$f \mapsto \chi_f,$$

which is in fact an isomorphism. Indeed, θ is injective, since we have supposed that $\operatorname{Ker}\chi \cap \mu_n(k) = \{1\}$. Hence, it is an isomorphism since Kummer theory shows that $(H : K^{*n}) = \operatorname{Card} G = \operatorname{Card} \hat{G}$.

(3.2) Proposition. *Let $f \in H/K^{*n}$, χ as in the beginning of this section, satisfying conditions (†), and $\mathscr{A}$ the Artin reciprocity map. We denote by γ the group of characters of the idele group I_K which are trivial on $K^* N_{L/K}(I_K)$. Then $\omega_f = \chi_f \circ \mathscr{A}$, and the map*

$$H/K^{*n} \to \gamma$$
$$f \mapsto \omega_f$$

is an isomorphism.

Proof. Let $z \in I_K$. Lemma (2.2.1) implies the first assertion. The second one follows from the exact sequence of Section (2.2) and from the isomorphism θ of Section (3.1). ■

(3.3) Proposition. *Let $u \notin U'(f)$, $f \equiv h \pmod{K^{*n}}$, with h regular at u, and χ as above, satisfying conditions (†). Then, if π_u is a local parameter at u,*

$$\omega_f(\pi_u) = \chi\big(N_{k(u)/k}(\overline{h(u)})\big)^{(q-1)/n}.$$

Proof. Proposition (3.2) shows that $\omega_f(\pi_u) = \chi_f(\mathscr{A} \circ j_u(\pi_u))$. But $\mathscr{A} \circ j_u(\pi_u) = \phi_u$ is the Frobenius of L/K at the place u (see [8, p. 297]). Hence

$$\omega_f(\pi_u) = \chi_f((\phi_u)) = \chi(\langle \phi_u, f \rangle) = \chi(\langle \phi_u, h \rangle).$$

Let $x \in L$ be such that $x^n = h$. Then by definition of the bracket, $\langle \phi_u, h \rangle = \phi_u x/x$. Letting $x(u)$ and $h(u)$ be the images of x and h in the residue field $k(u)$ of K_u, and $N(u)$ be the norm of u, we get

$$x(u)^n = h(u), \qquad \langle \phi_u, h \rangle = x(u)^{N(u)}/x(u).$$

So,

$$\begin{aligned} \langle \phi_u, h \rangle &= x(u)^{N(u)} \cdot \frac{x(u)^{N(u)/q}}{x(u)^{N(u)/q}} \cdots \frac{x(u)^q}{x(u)^q} \cdot \frac{1}{x(u)} \\ &= \frac{N_{k(u)/k}(x(u)^q)}{N_{k(u)/k}(x(u))} = N_{k(u)/k}(x(u)^{q-1}) = N_{k(u)/k}(h(u)^{(q-1)/n}), \end{aligned}$$

which proves the proposition. ■

(3.4) Let H_0 be a subgroup of K^*, containing K^{*n} as a subgroup of finite index, H_0 regular (cf. (1.3)). Let X and Y be respectively the smooth model of K and $L = K(H_0^{1/n})$. The extension L/K corresponds to a covering $\pi \colon Y \to X$, called a Kummer covering. Let χ be a character of k^* satisfying (†), so that $\gamma \approx \operatorname{Gal}(L/K)$ by Proposition (3.2). The following theorem computes the genus g_Y of Y:

(3.5) Theorem. *Let $r = (H_0\colon K^{*n})$, g_X and g_Y the genus of X and Y. Then*

$$2g_Y - 2 = r(2g_X - 2) + \sum_{f} \sum_{u \in U'(f)} \deg u,$$

where the first sum runs over a system of representatives of H_0/K^{*n}.

Proof. From the Hurwitz genus formula,

$$2g_Y - 2 = r(2g_X - 2) + \deg(\operatorname{discr}(L/K)),$$

since $[L:K] = r$ by Section (1.1). But the Führerdiskriminantenproduktformel ([5, p. 112]) states that

$$\operatorname{discr}(L/K) = \sum_{\omega \in \gamma} \mathfrak{f}(\omega),$$

where γ was defined in Proposition (3.2), and $\mathfrak{f}(\omega)$ was computed in Proposition (3.1). ■

IV. Character sums and L-functions.

(4.1) Notations are the same as in Section III. For $s \in \boldsymbol{N}^*$, let $k_s = \boldsymbol{F}_{q^s}$, and

$$\chi_s(x) = \chi(N_{k_s/k}(x)).$$

χ_s is a character of k_s^*. We can define, for $f \in K^*$ and $s \in \boldsymbol{N}^*$,

$$W(k_s, f) = \sum_{x \in X_*(k_s)} \chi_s(f(x))^{(q-1)/n},$$

where $X_*(k_s) = \{x \in X(k_s);\, f(x) \neq 0, \infty\}$. Let

$$X'(k_s) = \{x \in X(k_s);\, x \in \text{a place } u \text{ of } K \text{ s.t. } v'_u(f) \neq 0, \infty\}.$$

Then

$$X_*(k_s) \subset X'(k_s) \subset X(k_s).$$

Let $x \in X'(k_s)$, and suppose that $f = h \cdot g^n$, h non vanishing at x. We then define

$$\chi'_s(f(x)) = \chi_s(h(x)), \qquad W'(k_s, f) = \sum_{x \in X'(k_s)} \chi'_s(f(x))^{(q-1)/n}.$$

The L-function related to f is then defined as

$$L'(T, f) = \exp\left(\sum_{s=1}^{\infty} \frac{T^s}{s} W'(k_s, f)\right).$$

(4.2) On the other hand, the L-function related to a character ω of the idele class group $C_K = I_K/K^*$ of K is

$$L(T, \omega) = \prod_{u \notin R(\omega)} \frac{1}{1 - \omega(\pi_u) T^{\deg u}},$$

where π_u is a local parameter at the place u, and $R(\omega)$ is the ramification set of ω. The relation between the functions $L'(T, f)$ and $L(T, \omega)$ is the following:

(4.3) Proposition. *Let $f \in K^*$, χ a character of k^*, satisfying (†), and $L(T, \omega_f)$ the L-function related to the character $\omega_f \in \gamma$, γ being defined in Section (3.2). Then*

$$L'(T, \omega_f) = L(T, f).$$

Proof. Proposition (3.2) states that $\omega_f(\pi_u) = \chi\big(N_{k(u)/k}(\overline{h(u)})\big)^{(q-1)/n}$, where h is a regular representative of f modulo K^{*n}. On the other hand, a brief computation shows that

$$L(T, \omega_f) = \exp\left(\sum_{s=1}^{\infty} \frac{T^s}{s} V_s(f)\right),$$

with

$$V_s(f) = \sum_{u \notin R(\omega_f),\, \deg u | s} \deg u \cdot \omega_f(\pi_u)^{s/\deg u}.$$

But by Proposition (3.1), $U'(f) = R(\omega_f)$. So it is enough to prove that for $s \in \boldsymbol{N}^*$, we have $V_s(f) = W'(k_s, f)$. Let u be a place of K containing x; then $f(x) = f(u)$, and

$$\begin{aligned}\omega_f(\pi_u)^{s/\deg u} &= \chi\big(N_{k(u)/k}(\overline{h(u)}^{(q-1)/n})\big)^{s/\deg u} = \chi\big(N_{k_s/k}(\overline{h(u)})^{(q-1)/n}\big) \\ &= \chi_s(h(u))^{(q-1)/n} = \chi_s(\overline{f(u)})^{(q-1)/n} = \chi'_s(\overline{f(x)})^{(q-1)/n},\end{aligned}$$

and the proposition follows. ■

The zeta function $Z_X(T) = L(T, \omega_1)$, where ω_1 is the principal character, satisfies

$$Z_X(T) = \frac{P_X(T)}{(1-T)(1-qT)},$$

with $P_X(T) \in K_{2g_X - 2}[T]$.

(4.4) Corollary. *Let H_0 be a subgroup of K^* containing K^{*n} as a subgroup of finite index, and $L = K(H_0^{1/n})$. Call X and Y the nonsingular curves having K and L as function fields, and $\pi\colon Y \to X$ the corresponding covering. Choose a character χ of k^* satisfying (†). We denote by H' a system of representatives of the nonvanishing classes of H_0 (mod K^{*n}). Then*

$$Z_Y(T) = Z_X(T) \prod_{f \in H'} L'(T, f),$$

and

$$\# Y(k) - \# X(k) = \sum_{f \in H'} W'(k, f).$$

Proof. It is known ([6]) that

$$Z_Y(T) = \prod_{\omega \in \gamma} L(T, \omega),$$

with $\gamma = \{\omega_f;\, f \in H/K^{*n}\}$, which is isomorphic by Proposition (3.2) to H/K^{*n}. Hence, the first assertion follows from (3.2) and (4.3), and the second one from the first one, taking the logarithm of each side, and equating the coefficients of T in both sides. ∎

(4.5) Proposition. *Let $f \notin k^* K^{*n}$; then*

$$L'(T,f) = \sum_{i=1}^{C(f)} (1-\alpha_i(f)T), \quad \textit{with} \quad C(f) = 2g_X - 2 + \sum_{u \in U'(f)} \deg u;$$

$\alpha_i(f)$ are algebraic numbers, of modulus $\sqrt{q}$.

Moreover, for $s \geqslant 1$, we have

$$W'(k_s, f) = -\sum_{i=1}^{C(f)} \alpha_i(f)^s.$$

Proof. We have seen that $L'(T,f) = L(T,\omega_f)$. If ω_f is not the principal character, then $L(T,\omega_f)$ is a polynomial in T, of degree $2g_X - 2 + \deg \mathfrak{f}(\omega_f)$, where $\mathfrak{f}(\omega_f)$ was computed in Proposition (3.1) (see [8, p. 134]). Hence, $L'(T,f)$ is a polynomial of degree $C(f)$. The last part of the proposition follows from Riemann hypothesis for $Z_Y(T)$ (see [7]). ∎

(4.6) Corollary. *If $f \notin k^* K^{*n}$, then $|W'(k,f)| \leqslant C(f)\sqrt{q}$.*

Proof. This is clear. ∎

V. Bound for the number of points of a Kummer covering.

(5.1) Lemma (Serre). *Let $N \in \mathbf{N}^*$, and let $P(T) = \prod_{i=1}^{N}(1-\alpha_i T)$ be a polynomial of degree N, with coefficients in $\mathbf{Z}$, whose inverse roots α_i are of modulus $\sqrt{q}$. Then*

$$\Big|\sum_{i=1}^{N} (\alpha_i + \bar{\alpha}_i)\Big| \leqslant N[2\sqrt{q}].$$

In this lemma, $[x]$ denotes the integer part of x.

Proof Cf. [3, Lemma 4.1]. ∎

(5.2) Theorem. *Let H_0 be a nondegenerate subgroup of K^* containing K^{*n} as a subgroup of finite index, and H' a system of representatives of the nonvanishing classes of H_0 (mod K^{*n}). Then*

$$\Big|\sum_{f \in H'} W'(k,f)\Big| \leqslant \frac{B(H_0)}{2}[2\sqrt{q}],$$

with

$$B(H_0) = (r-1)(2g_X - 2) + \sum_{f \in H'} \sum_{u \in U'(f)} \deg u,$$

and $r = (H_0 : K^{*n})$.

Proof. Consider the Kummer covering $\pi\colon Y \to X$, and the polynomial (from Proposition 4.5)

$$\Lambda_q(T) = \prod_{f \in H'} L'(T,f) = Z_Y(T)/Z_X(T).$$

The Riemann hypothesis implies that $\Lambda_q(T)$ is a polynomial of degree $2g_Y - 2g_X$, that is, of degree $B(H_0)$ from Theorem (3.5). For $f \in H'$ and $1 \leqslant i \leqslant C(f)$, the algebraic number α_i satisfies $\alpha_i \cdot \bar{\alpha}_i = q$. The result now follows from Lemma (5.1). ∎

(5.3) Corollary. *Let $\pi\colon Y \to X$ be a Kummer covering. Then*

$$|\# Y(k) - \# X(k)| \leqslant \frac{B(H_0)}{2}[2\sqrt{q}].$$

Remark. This can be reformulated as

$$|\# Y(k) - \# X(k)| \leqslant (g_Y - g_X)[2\sqrt{q}].$$

This is an improvement, in this case, of Weil's inequality

$$|\# Y(k) - \# \boldsymbol{P}_1(k)| \leqslant g_Y[2\sqrt{q}].$$

The same estimate has been proved by Lachaud in the Artin–Schreier case (cf. [3]).

Proof. This is clear from Corollary (4.4) and Theorem (5.2). ∎

(5.4) Bound for traces. Let $\zeta_n = \exp(2i\pi/n)$. If $f \in K$, then $W'(k,f) \in \boldsymbol{Q}[\zeta_n]$, and if $F = \boldsymbol{Q}[\zeta_n]$, then $\mathrm{Gal}(F/\boldsymbol{Q}) = (\boldsymbol{Z}/n\boldsymbol{Z})^*$. Let

$$\varrho\colon (\boldsymbol{Z}/n\boldsymbol{Z})^* \to \mathrm{Gal}(F/\boldsymbol{Q})$$
$$c \mapsto \varrho_c,$$

ϱ_c being the $\boldsymbol{Q}$-automorphism of F given by $\varrho_c(\zeta_n) = \zeta_n^c$. On the other hand, $\varrho_c(W'(k,f)) = W'(k,f^c)$, so

(5.4.1) $$\mathrm{Tr}_{F/\boldsymbol{Q}}(W'(k,f)) = \sum_{c \in (\boldsymbol{Z}/n\boldsymbol{Z})^*} W'(k,f^c).$$

(5.5) Proposition. *If $f \notin k^* K^{*n}$, and if n is a prime number, then*

$$|\mathrm{Tr}_{F/\boldsymbol{Q}}(W'(k,f))| \leqslant (n-1)\frac{C(f)}{2}[2\sqrt{q}],$$

with

$$C(f) = 2g_X - 2 + \sum_{u \in U'(f)} \deg u.$$

Proof. Let H_0 be the subgroup of K^* generated by f and K^{*n}. A system of nonvanishing representatives of H/K^{*n} is $H' = \{f, f^2, \ldots, f^{n-1}\}$, that is, since n is prime, $H' = \{f^c\}_{c\in(\mathbf{Z}/n\mathbf{Z})^*}$. Then, by (5.4.1),

$$\mathrm{Tr}_{F/\mathbf{Q}}(W'(k,f)) = \sum_{g\in H'} W'(k,g),$$

and Theorem (5.2) enables us to write

$$|\mathrm{Tr}_{F/\mathbf{Q}}(W'(k,f))| = \frac{(r-1)(2g_X-2)+\sum_{c\in(\mathbf{Z}/n\mathbf{Z})^*}\sum_{u\in U'(f^c)}\deg u}{2}[2\sqrt{q}]$$

$$= (n-1)\frac{C(f)}{2}[2\sqrt{q}].$$

Since n is prime and $f\notin k^*K^{*n}$, hence $r = n$.

References

[1] N. Bourbaki, *Algèbre*, Chapitre V, Hermann, Paris 1981.
[2] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press, London 1963.
[3] G. Lachaud, *Artin–Schreier curves, exponential sums and the Carlitz–Uchiyama bound for geometric codes*, J. Number Theory, to appear.
[4] S. Lang, *Algebra*, 2nd ed., Addison-Wesley, Reading 1984.
[5] J. P. Serre, *Corps locaux*, Actualités scientifiques et industrielles, Publ. Inst. Math. Univ. Nancago VIII, 1296, Hermann, Paris 1962.
[6] —, *Zeta and L-functions*, Arithmetical Algebraic Geometry, Harper and Row, New York 1965, 82–92; = Oeuvres, t. II, n° 64, Springer, Berlin 1986, 249–259.
[7] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Publ. Inst. Math. Univ. Strasbourg VII, [1948c], Springer, Berlin 1979.
[8] —, *Basic Number Theory*, Springer, New York 1967.

EQUIPE C.N.R.S. ARITHMÉTIQUE ET THÉORIE DE L'INFORMATION
C.I.R.M. Luminy Case 916
13288 Marseille Cedex 9
France

Received on 28.6.1990 (2057)

ACTA ARITHMETICA
LIX.3 (1991)

Symmetric Diophantine systems

by

AJAI CHOUDHRY (Singapore)

1. Introduction. In this paper we will consider symmetric Diophantine systems in $2n$ independent variables x_j, $j = 1, 2, \ldots, n$, and y_j, $j = 1, 2, \ldots, n$, consisting of a set of simultaneous Diophantine equations of the type

$$f_i(x_1, x_2, \ldots, x_n) = f_i(y_1, y_2, \ldots, y_n), \qquad i = 1, 2, \ldots, m, \tag{1.1}$$

where $f_i(x_1, x_2, \ldots, x_n)$ [written briefly as $f_i(x_j)$ or simply as f_i] is, for each i, a homogeneous form in the variables $x_1, x_2, \ldots, x_n$. We shall describe a method that can be applied to solve several such Diophantine systems. The solutions obtained are parametric but, unless otherwise stated, are not necessarily complete. We shall use L's, Q's, C's and F's to denote linear, quadratic, cubic and quartic forms. We shall first solve under quite general conditions the following Diophantine systems in $2n$ variables x_j, y_j, $j = 1, 2, \ldots, n$:

$$\text{(I)} \qquad \begin{cases} L_i(x_j) = L_i(y_j), & i = 1, 2, \ldots, n-1, \\ Q_i(x_j) = Q_i(y_j), & i = 1, 2, \ldots, n-1. \end{cases}$$

$$\text{(II)} \qquad \begin{cases} L_i(x_j) = L_i(y_j), & i = 1, 2, \ldots, n-2, \\ C(x_j) = C(y_j). \end{cases}$$

A particular case of interest is the system

$$\begin{cases} L(x_1, x_2, x_3) = L(y_1, y_2, y_3), \\ C(x_1, x_2, x_3) = C(y_1, y_2, y_3). \end{cases}$$

$$\text{(III)} \qquad \begin{cases} Q_i(x_j) = Q_i(y_j), & i = 1, 2, \ldots, n-2, \\ C(x_j) = C(y_j). \end{cases}$$

A particular case of interest is the system

$$\begin{cases} Q(x_1, x_2, x_3) = Q(y_1, y_2, y_3), \\ C(x_1, x_2, x_3) = C(y_1, y_2, y_3). \end{cases}$$

$$\text{(IV)} \qquad \begin{cases} L_i(x_j) = L_i(y_j), & i = 1, 2, \ldots, n-2, \\ Q_i(x_j) = Q_i(y_j), & i = 1, 2, \ldots, k < n/2, \\ C(x_j) = C(y_j). \end{cases}$$