Multiplicative character sums and Kummer coverings

by

MARC PERRET (Marseille)

0. Introduction. Let $k = F_q$ be the finite field with $q$ elements, $\chi$ 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 $\pi: Y \to X$; 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 $n$th roots of unity. Let $r$ be the lowest integer such that $a^r \in K^*$. Then the subfield $L$ of a given algebraic closure $\Omega$ 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 $K^{**}$. For each $a \in H/K^{**}$, let $\theta_a \in \Omega$ be such that $\theta_a^r$ represents $a$ in $H$ modulo $K^{**}$. 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,
\[ \text{Gal}(K(H^{1/n})/K) \cong H/K^{*n}, \]
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 \(H \rightarrow K(H^{1/n})\) is an increasing one-to-one mapping from the set of subgroups of \(K^{*}\) containing \(K^{*n}\) onto the set of abelian subextensions of \(\Omega\), whose exponent divides \(n\) (cf. [1, p. 85]).

Let \(G\) be the Galois group \(\text{Gal}(K(H^{1/n})/K)\). If \(\sigma \in G\) and \(h \in H\), then there exists \(x \in K(H^{1/n})\) such that \(x^a = h\); we can then define
\[ \langle \sigma, h \rangle = \frac{\sigma(x)}{x} \in \mu_a(K). \]

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

\[ G \times H/K^{*n} \rightarrow \mu_a(K). \]

(1.2) Let \(X\) be a smooth irreducible projective curve defined over a finite field \(k\), and let \(K = \mathbb{R}(X)\) 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 \(F\) is an algebraic closure of \(k\):

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

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

(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 \(\bar{K}^{*n} \cap H_0 = K^{*n}\).

Proof. Let \(\tilde{H} = H_0 \tilde{K}^{*n}\). There is a canonical surjective morphism
\[ \varphi: K(H^{1/n}) \otimes_k F \rightarrow \tilde{K}(H^{1/n})]. \]

hence \(K(H^{1/n}) \otimes_k F\) is a field if and only if \(\varphi\) is an isomorphism. But
\[ [K(H^{1/n}) \otimes_k F; \tilde{K}] = (\tilde{H}; \tilde{K}^{*n}] = (H_0; \tilde{K}^{*n} \cap H_0). \]

\[ K(H^{1/n}) \otimes_k F\) is a field \(\iff (H_0; \tilde{K}^{*n} \cap H_0) = (H_0; K^{*n}) \iff \tilde{K}^{*n} \cap H_0 = K^{*n}. \]

So,
\[ K(H^{1/n}) \otimes_k F\) is a field \(\iff (H_0; \tilde{K}^{*n} \cap H_0) = (H_0; K^{*n}) \iff \tilde{K}^{*n} \cap H_0 = K^{*n}. \]

since we always have \(K^{*n} \subseteq \tilde{K}^{*n} \cap H_0. \)

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 \(K(H^{1/n})/K\) is regular.

(1.4) Let \(k = \mathbb{F}_q\) be the finite field with \(q\) elements, \(K\) a function field of one variable over \(k\), and \(n \geq 2\) an integer such that \(n \mid q - 1\) (then \(K\) contains the group of \(n^{th}\) 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
\[ v_u(f) = \min_{\sigma \in K^{*}} (|v_u(f\sigma)|) \]

where \(|x|\) is the absolute value of \(x \in \mathbb{R}\), therefore
\[ v_u(f) = 0 \iff f \in \mathcal{O}_u \cdot K^{*n}, \]
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
\[ f = h \pmod{K^{*n}} \]
and \(0 \leq v_u(h) < n\).

Moreover,
\[ v_u(f) = v_u(h). \]
In particular, \(0 \leq v_u(f) < n\).

Proof. If \(f \in K^{*}\), let \(\pi\) be a local parameter at the place \(u\). Since \(v_u(f)\) is defined by an absolute value, we can suppose that \(v = v_u(f) \geq 0\). So we can write \(f\) as
\[ f = \sum_{i=0}^{\infty} a_i \pi^i. \]

If \(n \geq n\), let \(v = an + r\) with \(0 \leq r < n\) be the division of \(v\) by \(n\), and define \(g = n^{-a}\); then
\[ f \pi^r = a_i \pi^i + \sum_{i>r} b_i \pi^i \]
and \(v_u(f \pi^r) = r\), which shows that
\[ 0 \leq v_u(f) \leq v_u(f \pi^r) = r < n. \]

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

$$\left( a, b \right)_u = N_{k(u)/k}^\times \left( (-1)^{a_u b_u} a_u^{-1} b_u^{-1} \right) \in \mu_n(k),$$

where $\alpha$ and $\beta$ are as defined before.

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

$$1 \to K^*_u N_{L/K}(L^\times) \to I_K \to G \to 1$$

is exact (see [2]).

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

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

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

$$\left( f, x_{\bar{u}} \right) = \left( x_{f, u}, x_{u_{\bar{u}}} \right) \in \mu_n(K), \quad \langle \sigma(f), x \rangle = \prod_{u} \langle f, x_u \rangle.$$  

Proof. For every character $x \in \text{Hom}(G, \mathbb{Q}/\mathbb{Z})$, and for every idele $z \in I_K$,

$$x \circ \sigma(z) = \prod_{u} \text{Inv}_{K_u}(x_{f, u} \circ x_{u, u_{\bar{u}}}, z_{u_{\bar{u}}}) \in \mathbb{Q}/\mathbb{Z}$$

([2, p. 189]). Hence, if $x$ is a primitive $n$-root of unity in $K$, (2.2.2)

$$x^{q-1} \in \mu_n(\mathbb{Q}/\mathbb{Z}) = \prod_{u} \text{Inv}_{K_u}(x_{f, u} \circ x_{u, u_{\bar{u}}}, z_{u_{\bar{u}}}).$$

If $x_{f, u} \in \text{Hom}(G, \mathbb{Q}/\mathbb{Z})$ is the character associated to $f$, then ([5, p. 213])

$$\langle \sigma, f \rangle = \omega^{x_{f, u} \circ x_{u, u_{\bar{u}}}}.$$  

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

III. The genus of a Kummer covering. We make the same assumptions as in (2.2). Let $\chi \in \text{Hom}(G, \mathbb{Q}/\mathbb{Z})$ be a character of the multiplicative group of $k = F_q$, and let $u$ be a place of $K$. In all this paper, we shall assume that the following assumptions hold:

1. $\ker \chi \circ \mu_n(k) = \{1\}$ and $\chi^{(q-1)/n} \neq 1$ for every place $u$ of $K$.

Such a character always exists, we can choose for example a generator $\chi$ of the cyclic group $K^*$.

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

$$K^*_u / K^*_u \times K^*_u / K^*_u \to \mu_n(k).$$
For $a, b \in K^*_u$, 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 $f \in K^*$,
\[ \omega_f(z) = \prod_u (f, z_u). \]
Note that $\omega_f$ depends on $\chi$.

(3.1) Proposition. Suppose that $\chi$ satisfies conditions (†), and let $U'(f)$ be the set of places $u$ of $K$ such that $\nu_u(f) > 0$. Then the ramification set $R(\omega_f)$ of $\omega_f$ is equal to $U'(f)$, and its conductor is given by
\[ t(\omega_f) = \sum_{u \in U'(f)} u. \]

Proof. If $u$ is a place of $K$, let $\mathcal{O}_u$ be the ring of regular functions at $u$, and $p_u$ its maximal ideal. We write $\omega_u(z)$ instead of $(f, z_u)$, for every $z \in K^*_u$. By definition of the conductor, $t(\omega_f) = \sum u_i$, where $u_i$ is the smallest integer $k \geq 0$ such that $\omega_u(z) = 1$ for every $z \equiv 1 \pmod{p_u}$.

Let $f \equiv h \pmod{K^*}$, with $h \in \mathcal{O}_u^*$, such that $\nu_u(f) = \nu_u(h) = v$. Then $f = g^v \cdot h$, $g \in K^*$ and, if $z \in \mathcal{O}_u^*$,
\[ (f, z)_u = (h, z_u) = N_{k(u)}(\bar{z}) \zeta(v, z)^{v-1}, \]
with $x = v(h) = v$ and $\beta = v_u(z) = 0$. Hence,
\[ (f, z)_u = N_{k(u)}(\bar{z})^{-v-1}. \]

There are two cases:
- If $u \not\in U'(f)$, then $v = 0$, and $(f, z)_u = 0$, so $t_u = 0$.
- If $u \in U'(f)$, since $\chi^{\nu-1} = \chi(1) \not\equiv 1$, we have $t_u \geq 1$. On the other hand, if $z \equiv 1 \pmod{p_u}$, then $z = 1$, so $(f, z)_u = 0$, and $t_u = 1$, which proves the proposition.

Let $H$ be a subgroup of $K^*$, containing $K^*$ as a subgroup of finite index.

Kummer theory gives (see (1.1)) a non-degenerate bilinear mapping
\[ G \times H/K^* \rightarrow \mu_k(k) \]
\[ (\sigma, h) \mapsto <\sigma, h>. \]

For $f \in K^*$, we consider the character $\chi_f \in \mathcal{G}$ associated to $f$ by class field theory (cf. § II)
\[ \chi_f: G \rightarrow C^* \]
\[ f \mapsto \chi_f. \]

This defines a morphism
\[ 0: H/K^* \rightarrow \mathcal{G} \]
\[ f \mapsto \chi_f, \]
which is in fact an isomorphism. Indeed, $\delta$ is injective, since we have supposed that $\text{Ker}\chi \cap \mu_k(k) = \{1\}$. Hence, it is an isomorphism since Kummer theory shows that $(H: K^*) = \text{Card} \mathcal{G} = \text{Card} \mathcal{G}$.

(3.2) Proposition. Let $f \in H/K^*$, $\chi$ as in the beginning of this section, satisfying conditions (†), and $\mathcal{A}$ the Artin reciprocity map. We denote by $\gamma$ the group of characters of the idele group $I_K$ which are trivial on $K^* N_{L/K}(I_K)$. Then $\omega_f = \chi_f \circ \mathcal{A}$, and the map
\[ H/K^* \rightarrow \gamma \]
\[ f \mapsto \omega_f \]
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 $\theta$ of Section (3.1).

(3.3) Proposition. Let $u \not\in U'(f)$, $f \equiv h \pmod{K^*}$, with $h$ regular at $u$, and $\chi$ as above, satisfying conditions (†). Then, if $\pi_u$ is a local parameter at $u$,
\[ \omega_f(\pi_u) = \chi(N_{k(u)/k}(h(u)))^{\frac{1}{q-1}}, \]
\[ \text{and} \mathcal{A}(\pi_u) = \chi_f(\phi_u) = (\chi(\phi_u), f) = \chi(\phi_u, h). \]

Proof. Proposition (3.2) shows that $\omega_f(\pi_u) = \chi_f(\phi_u, f)$, $\mathcal{A}(\pi_u) = \chi_f(\phi_u, f)$, but $\mathcal{A}(\phi_u, f) = \chi(\phi_u, h)$. Let $x \in L$ be such that $x^q = h$. Then by definition of the bracket, $\langle \phi_u, h \rangle = \phi_u x^q$. 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
\[ x(u)^q = h(u), \quad \langle \phi_u, h \rangle = x(u)^{q-1} / x(u). \]
So,
\[ N_{k(u)/k}(x(u)) = \frac{N_{k(u)/k}(x(u^q))}{x(u)^q} = \frac{N_{k(u)/k}(x(u))}{x(u)^q} = \frac{N_{k(u)/k}(x(u))}{x(u)^{q-1}} = N_{k(u)/k}(h(u)^{q-1}), \]
which proves the proposition.

(3.4) Let $H_0$ be a subgroup of $K^*$, containing $K^*$ as a subgroup of finite index, $H_0$ regular (cf. (1.3)). Let $X$ and $Y$ be respectively the smooth model of $K$ and $L = K(H_0^*)$. The extension $L/K$ corresponds to a covering $\pi: Y \rightarrow X$, called a Kummer covering. Let $\chi$ be a character of $k^*$ satisfying (†), so that $\pi \cong \text{Gal}(L/K)$ by Proposition (3.2). The following theorem computes the genus $g_Y$ of $Y$.
(3.5) Theorem. Let \( r = (H_0; K^{*}) \), \( g_x \) and \( g_y \) the genus of \( X \) and \( Y \). Then
\[
2g_Y - 2 = r(2g_X - 2) + \sum_{T \in U(T)} \deg u,
\]
where the first sum runs over a system of representatives of \( H_0/K^{*} \).

Proof. From the Hurwitz genus formula,
\[
2g_Y - 2 = r(2g_X - 2) + \deg \text{disc}(L/K),
\]
since \([L:K] = r\) by Section (1.1). But the Führerdiskriminantenproduktformel ([5, p. 112]) states that
\[
\text{disc}(L/K) = \sum_{\omega \in \gamma} t(\omega),
\]
where \( \gamma \) was defined in Proposition (3.2), and \( t(\omega) \) was computed in Proposition (3.1).

IV. Character sums and L-functions.

(4.1) Notations are the same as in Section III. For \( s \in N^{*} \), let \( k_s = F_{q^s} \), and
\[
\chi_s(x) = \chi(N_{k_s/k}(x)).
\]
where \( \chi_s \) is a character of \( k_s^{*} \). We can define, for \( f \in K^{*} \) and \( s \in N^{*} \),
\[
W(k_s, f) = \sum_{x \in X(k_s)} \chi_s(f(x))^{q^{s-1}/n},
\]
where \( X(k_s) = \{ x \in X(k_s); f(x) \neq 0, \infty \} \). Let
\[
X'(k_s) = \{ x \in X(k_s); x \in \text{a place } u \text{ of } K \text{ s.t. } \nu_u(f) \neq 0, \infty \}.
\]
Then
\[
X_s(k_s) \subset X'(k_s) \subset X(k_s).
\]
Let \( x \in X'(k_s) \), and suppose that \( f = h \circ g_s \), \( h \) non vanishing at \( x \). We then define
\[
\chi_s(f(x)) = \chi_s(h(x)), \quad W'(k_s, f) = \sum_{x \in X'(k_s)} \chi_s(f(x))^{q^{s-1}/n}.
\]

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 \( \omega \) of the idele class group \( C_K = K^{*} \) of \( K \) is
\[
L(T, \omega) = \prod_{u \in R(\omega)} \frac{1}{1 - \omega(\pi_u)T^{\deg u}},
\]
where \( \pi_u \) is a local parameter at the place \( u \), and \( R(\omega) \) is the ramification set of \( \omega \). The relation between the functions \( L(T, f) \) and \( L(T, \omega) \) is the following:

(4.3) Proposition. Let \( f \in K^{*} \), \( \chi \) a character of \( k^{*} \), satisfying (1), and \( L(T, \omega) \) the L-function related to the character \( \omega \), \( \gamma \) being defined in Section (3.2). Then
\[
L(T, \omega) = \frac{1}{1 - h(\mu)(\omega(f))^{q - 1}/n}.
\]

Proof. Proposition (3.2) states that \( \omega(f)(\mu) = \chi(N_{k_{10}/k}(h(\mu)))^{q^{s-1}/n} \), where \( h \) is a regular representative of \( f \) modulo \( K^{*} \). On the other hand, a brief computation shows that
\[
L(T, \omega) = \exp \left( \sum_{s=1}^{\infty} \frac{T^s}{s} V_s(f) \right),
\]
with
\[
V_s(f) = \sum_{u \in R(\omega), \deg u \leq s} \deg u \omega(f(u))^{q^{s-1}/n},
\]
but by Proposition (3.1), \( U'(f) = R(\omega) \). So it is enough to prove that for \( s \in N^{*} \), we have \( V_s(f) = W'(k_s, f) \). Let \( u \) be a place of \( K \) containing \( x \); then \( f(x) = u(f) \), and
\[
\omega(f)(\mu) = \chi(N_{k_{10}/k}(h(\mu)))^{q^{s-1}/n} = \chi(N_{k_{10}/k}(h(\mu)))^{q^{s-1}/n},
\]
and the proposition follows.

The zeta function \( Z_x(T) = L(T, \omega) \), where \( \omega_1 \) is the principal character, satisfies
\[
Z_x(T) = \frac{P_x(T)}{(1 - T)(1 - qT)},
\]
with \( P_x(T) \in K_{2x-2}[T] \).

(4.4) Corollary. Let \( H_0 \) be a subgroup of \( K^{*} \) containing \( K^{*} \) as a subgroup of finite index, and \( L = K(\mathbb{H})^{*} \). Call \( X \) and \( Y \) the nonsingular covering fields of \( K \) and \( L \) as function fields, and \( \pi_1 ; X \rightarrow Y \) the corresponding covering. Choose a character \( \chi \) of \( k^{*} \) satisfying (1). We denote by \( H \) a system of representatives of the nonvanishing classes of \( H_0 \) modulo \( K^{*} \). 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
\[
Z_x(T) = \prod_{\omega \in \gamma} L(T, \omega),
\]
with $\gamma = \{\omega_f ; f \in H/K^*\}$, which is isomorphic by Proposition (3.2) to $H/K^*$. 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

$$L(T, f) = \sum_{i=1}^{c(f)} (1 - \alpha_i(f)) T,$$

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

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

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

$$W_s(k, f) = -\sum_{i=1}^{c(f)} \alpha_i(f)^s.$$

Proof. We have seen that $L(T, f) = L(T, \omega_f)$. If $\omega_f$ is not the principal character, then $L(T, \omega_f)$ is a polynomial in $T$, of degree $2g_x - 2 + \deg l(\omega_f)$, where $l(\omega_f)$ 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 $Z_T(T)$ (see [7]).

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

Proof. This is clear.

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

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

$$\sum_{i=1}^{N} (\alpha_i + \bar{\alpha_i}) \leq N \sqrt{2q}.$$

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 $K^*$). Then

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

with

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

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

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

$$A_q(T) = \prod_{f \in H} L(T, f) = Z_T(T)/Z_X(T).$$

The Riemann hypothesis implies that $A_q(T)$ is a polynomial of degree $2g_x - 2 + \deg l(\omega_f)$, that is, of degree $B(H_0)$ from Theorem (3.5). For $f \in H'$ and $1 \leq i \leq C(f)$, the algebraic number $\alpha_i$ satisfies $\alpha_i, \bar{\alpha}_i \in q$. The result now follows from Lemma (5.1).

(5.3) COROLLARY. Let $\pi : Y \to X$ be a Kummer covering. Then

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

Remark. This can be reformulated as

$$|\# Y(k) - \# X(k)| \leq (g_y - g_x) [2\sqrt{q}].$$

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

$$|\# Y(k) - \# X(k)| \leq g_x [2\sqrt{q}].$$

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 $\zeta_n = \exp(2\pi i/n)$. If $f \in K$, then $W(k, f) \in Q[\zeta_n]$, and if $F = Q[\zeta_n]$, then $Gal(F/Q) = \langle (Z/nZ)^* \rangle$. Let $\varpi : (Z/nZ)^* \to Gal(F/Q)$

$$c \mapsto \varpi(c),$$

$\varpi$, being the $Q$-automorphism of $F$ given by $\varpi(\zeta_n) = \zeta_n$. On the other hand, $\varpi(W(k, f)) = W(k, f)$, so

$$[\text{Tr}_{F/Q}(W(k, f))] = \sum_{c \in (Z/nZ)^*} W(k, f).$$

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

$$[\text{Tr}_{F/Q}(W(k, f))] \leq \frac{B(H_0)}{2} (n-1) [2\sqrt{q}],$$

with

$$C(f) = 2g_x - 2 + \sum_{u \in U(f)} \deg u.$$
that is, since $n$ is prime, $H' = \{ f' \}_{f \in \mathbb{Z}/n\mathbb{Z}}$. Then, by (5.4.1),
\[
\text{Tr}_{F_{Q}}(W'(k, f)) = \sum_{g \in H'} W'(k, g),
\]
and Theorem (5.2) enables us to write
\[
|\text{Tr}_{F_{Q}}(W'(k, f))| = \frac{(r-1)(2d-2) + \sum_{f \in \mathbb{Z}/n\mathbb{Z}} \sum_{g \in H'} |f| \deg u}{2} [2\sqrt{q}]
\]
\[
= (n-1) \frac{C(f)}{2} [2\sqrt{q}].
\]
Since $n$ is prime and $f \neq k^* K^*$, hence $r = n$.

References


Symmetric Diophantine systems
by
AJAI CHOUDHRY (Singapore)

1. Introduction. In this paper we will consider symmetric Diophantine systems in $2n$ independent variables $x_j, y_j, j = 1, 2, \ldots, n$, and $y_j, y_j, j = 1, 2, \ldots, n$, consisting of a set of simultaneous Diophantine equations of the type
\[
f_i(x_1, x_2, \ldots, x_n) = f_i(y_1, y_2, \ldots, y_n), \quad i = 1, 2, \ldots, m,
\]
where $f_i(x_1, x_2, \ldots, x_n)$ is a polynomial 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 $x_j, y_j, j = 1, 2, \ldots, n$:

\[
\begin{align*}
(1) \quad & \begin{cases} 
L_1(x_1, x_2, x_3) = L_1(y_1, y_2, y_3), \\
C(x_1, x_2, x_3) = C(y_1, y_2, y_3).
\end{cases} \\
(2) \quad & \begin{cases} 
L_2(x_1, x_2, x_3) = L_2(y_1, y_2, y_3), \\
C(x_1, x_2, x_3) = C(y_1, y_2, y_3).
\end{cases}
\end{align*}
\]

A particular case of interest is the system
\[
\begin{align*}
& \begin{cases} 
Q_1(x_1, x_2, x_3) = Q_1(y_1, y_2, y_3), \\
C(x_1, x_2, x_3) = C(y_1, y_2, y_3).
\end{cases} \\
& \begin{cases} 
Q_2(x_1, x_2, x_3) = Q_2(y_1, y_2, y_3), \\
C(x_1, x_2, x_3) = C(y_1, y_2, y_3).
\end{cases}
\end{align*}
\]

A particular case of interest is the system
\[
\begin{align*}
& \begin{cases} 
Q_1(x_1, x_2, x_3) = Q_1(y_1, y_2, y_3), \\
C(x_1, x_2, x_3) = C(y_1, y_2, y_3).
\end{cases} \\
& \begin{cases} 
Q_2(x_1, x_2, x_3) = Q_2(y_1, y_2, y_3), \\
C(x_1, x_2, x_3) = C(y_1, y_2, y_3).
\end{cases}
\end{align*}
\]