[11] E. S. Selmer, *Linear recurrence relations over finite fields*, University of Bergen, 1966.
[12] D. Singmaster, *Divisibility of binomial coefficients by primes and prime powers*, available from the author, Polytechnic of the South Bank, London 1974.
[13] J. Touchard, *Proprietes arithmetiques de certains nombres recurrents*, Ann. Soc. Sci. Bruxelles 53A (1933), pp. 21–31.
[14] — *Nombres exponentiels et nombres de Bernoulli*, Canad. J. Math. 8 (1956), pp. 305–320.
[15] G. T. Williams, *Numbers generated by the function* e^{e^z-1}, Amer. Math. Monthly 52 (1945), pp. 323–327.

Received on 4. 3. 1975
and in revised form on 3. 12. 1976 (685)

ACTA ARITHMETICA
XXXV (1979)

Gauss sums and solutions to simultaneous equations over GF(2^y)

by

JOHN D. FULTON (Clemson, S.C.)

1. Introduction. Let $q = 2^y$, $y \geqslant 1$, and let $F = \mathrm{GF}(q)$, the finite field of order q. For $a \in F$, $t(a) = a + a^2 + \ldots + a^{2^{y-1}}$ defines a homomorphism t of the additive group $(F, +)$ onto the additive group of the prime subfield $\{0, 1\}$ of F, and $e(a) = e^{2\pi i t(a)}$ defines a homomorphism e of $(F, +)$ onto the multiplicative group of integers $\{1, -1\}$([3], p. 29).

Thus, it can be seen that

$$\sum_x e(ax) = \begin{cases} q, & a = 0, \\ 0, & a \neq 0. \end{cases} \tag{1.1}$$

Let $F^{1\times s}$ denote the vector space over F consisting of vectors $\chi = (x_1, x_2, \ldots, x_s)$. Let Q be a quadratic form of full rank s on $F^{1\times s}$ and let g be its associated bilinear form. Then there exists a basis for $F^{1\times s}$ ([3], p. 197) such that if $\chi = (x_1, x_2, \ldots, x_s) \in F^{1\times s}$, then $Q(\chi)$ equals precisely one of the following

$$x_1x_{k+1} + x_2x_{k+2} + \ldots + x_kx_{2k} + x_{2k+1}^2, \qquad s = 2k+1, \tag{1.2}$$

$$x_1x_{k+1} + x_2x_{k+2} + \ldots + x_kx_{2k}, \qquad s = 2k, \tag{1.3}$$

$$x_1x_{k+1} + x_2x_{k+2} + \ldots + x_kx_{2k} + x_{2k+1}^2 + x_{2k+1}x_{2k+2} + \beta x_{2k+2}^2, \qquad s = 2k+2, \tag{1.4}$$

where in (1.4), β is any element of F such that the polynomial $u^2 + uv + \beta v^2$ is irreducible in the polynomial ring $F[u, v]$.

We say that quadratic form Q has type $\tau = 0, 1$, or -1 according as Q is equivalent under change of basis for $F^{1\times s}$ to (1.2), (1.3), or (1.4), respectively.

Similarly, under any change of basis for $F^{1\times s}$ which produces one of the forms (1.2), (1.3), or (1.4) for Q, for $\xi = (b_1, b_2, \ldots, b_s)$ and $\chi = (x_1, x_2, \ldots, x_s)$ in $F^{1\times s}$, $g(\xi, \chi)$ equals

(1.5) $$b_1x_{k+1} + \ldots + b_kx_{2k} + b_{k+1}x_1 + \ldots + b_{2k}x_k \quad \text{if} \quad \tau = 0 \ (s = 2k+1),$$

(1.6) $$b_1x_{k+1} + \ldots + b_kx_{2k} + b_{k+1}x_1 + \ldots + b_{2k}x_k \quad \text{if} \quad \tau = 1 \ (s = 2k),$$

(1.7) $$b_1x_{k+1} + \ldots + b_kx_{2k} + b_{k+1}x_1 + \ldots + b_{2k+1}x_k + b_{2k+1}x_{2k+2} + b_{2k+2}x_{2k+1} \quad \text{if} \quad \tau = -1 \ (s = 2k+2).$$

Thus, if $\tau = 0$, g is less than full rank; while if $\tau = \pm 1$, g is of full rank s.

For arbitrary t, u, v in F, we shall determine the number $N(s; t, u, v)$ of solutions $(\xi, \chi) \in F^{1\times s} \times F^{1\times s}$ to the system of simultaneous equations

(1.8) $$Q(\xi) = t,$$

(1.9) $$Q(\chi) = u,$$

and

(1.10) $$g(\xi, \chi) = v.$$

If $\chi = (x_1, x_2, \ldots, x_s)$ and $Q(\chi) = \sum_{i\leqslant j} a_{ij}x_ix_j$, then $Q(\chi) = \chi A \chi^T$, where $A = (a_{ij})$ is upper triangular. Moreover, if $\xi = (b_1, b_2, \ldots, b_s)$, $g(\xi, \chi) = \xi(A + A^T)\chi^T$. Let P be the matrix of change of basis for $F^{1\times s}$ which takes Q to one of the forms (1.2), (1.3), or (1.4) and g to the corresponding form (1.5), (1.6), or (1.7).

Hence, for $s = 2k+l$,

$$Q(\xi) = \xi A \xi^T = (\xi P^{-1})PAP^T(\xi P^{-1})^T = (\xi P^{-1})G_{2k+l}(\xi P^{-1})^T = Q_0(\xi P^{-1});$$
$$Q(\chi) = (\chi P^{-1})G_{2k+l}(\chi P^{-1})^T = Q_0(\chi P^{-1});$$

and

$$g(\xi, \chi) = \xi(A + A^T)\chi^T = (\xi P^{-1})P(A + A^T)P^T(\chi P^{-1})^T$$
$$= (\xi P^{-1})F_{2k+l}(\chi P^{-1})^T = g_0(\xi P^{-1}, \chi P^{-1}),$$

where if $l = 1$, Q_0 has the form (1.2), g_0 has the form (1.5),

$$G_{2k+1} = \begin{bmatrix} 0 & I_k & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad F_{2k+1} = G_{2k+1} + G_{2k+1}^T,$$

if $l = 0$, Q_0 has the form (1.3), g_0 has the form (1.6),

$$G_{2k} = \begin{bmatrix} 0 & I_k \\ 0 & 0 \end{bmatrix}, \quad F_{2k} = G_{2k} + G_{2k}^T,$$

and if $l = 2$, Q_0 has the form (1.4), g_0 has the form (1.7),

$$G_{2k+2} = \begin{bmatrix} 0 & I_k & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & \beta \end{bmatrix}, \quad F_{2k+2} = G_{2k+2} + G_{2k+2}^T.$$

The superscript T denotes transpose, and I_k denotes the $k\times k$ identity matrix.

Since P^{-1} is an isomorphism of vector space $F^{1\times s}$, the number solutions (ξ, χ) to the system of simultaneous equations defined by (1.8), (1.9), and (1.10) is precisely the number of solutions to the system

(1.11) $$Q_0(\xi) = t,$$

(1.12) $$Q(\chi) = u,$$

(1.13) $$g_0(\xi, \chi) = v,$$

where Q_0 is given by one of the equations (1.2), (1.3), (1.4) and the corresponding g_0 is given by one of the equations (1.5), (1.6), (1.7). Therefore we seek the number $N(s; t, u, v)$ of solutions $(\xi, \chi) \in F^{1\times s}$ to the system defined by (1.11), (1.12), and (1.13).

In determining $N(s; t, u, v)$, we use results established by Carlitz ([1], [2]) concerning Gauss, or exponential sums defined for equations over $F = \mathrm{GF}(2^\nu)$.

2. Enumeration of solutions to $Q_0(\xi) = t$. Let $N_1(s; t)$ denote the number of solutions $\xi = (b_1, b_2, \ldots, b_s)$ to (1.11). Then from (1.1),

(2.1) $$qN_1(s; t) = \sum_{\xi}\sum_{c} e\{c(Q_0(\xi) + t)\} = \sum_{c} e(ct) \sum_{\xi} e(cQ_0(\xi)).$$

If $s = 2k+1$, then from (1.2),

$$Q_0(\xi) = \sum_{i=1}^{k} b_ib_{k+i} + b_{2k+1}^2,$$

and (2.1) becomes

(2.2) $$qN_1(2k+1, t) = \sum_{c} e(ct) \sum_{b_{2k+1}} e(cb_{2k+1}^2) \prod_{i=1}^{k} \sum_{b_i} \sum_{b_{k+i}} e(cb_ib_{k+i})$$
$$= q^{2k+1} + \sum_{c\neq 0} e(ct) \sum_{b_{2k+1}} e(cb_{2k+1}^2) \prod_{i=1}^{k} \sum_{b_i} \sum_{b_{k+i}} e(cb_ib_{k+i}).$$

Let $y = ab_{2k+1}$, where $a^2 = c$ in F. Hence, in (2.2),

(2.3) $$\sum_{b_{2k+1}} e(cb_{2k+1}^2) = \sum_{y} e(y^2) = \sum_{y} e(y) = 0,$$

by (1.1), since squaring permutes F. Thus, by applying (2.3) to (2.2), we obtain

$$N_1(2k+1, t) = q^{2k} = q^{s-1}. \tag{2.4}$$

If $s = 2k$, then from (1.3),

$$Q_0(\xi) = \sum_{i=1}^{k} b_i b_{k+i},$$

and (2.1) becomes

$$\begin{aligned} qN_1(2k, t) &= \sum_{c} e(ct) \prod_{i=1}^{k} \sum_{b_i} \sum_{b_{k+i}} e(cb_i b_{k+i}) \\ &= q^{2k} + \sum_{c\neq 0} e(ct) \prod_{i=1}^{k} \sum_{b_i} \sum_{b_{k+i}} e(cb_i b_{k+i}) \\ &= q^{2k} + q^k \sum_{c\neq 0} e(ct). \end{aligned} \tag{2.5}$$

Now from (1.1),

$$\sum_{c\neq 0} e(ct) = \begin{cases} q-1 & \text{if} \quad t = 0, \\ -1 & \text{if} \quad t \neq 0. \end{cases} \tag{2.6}$$

Thus,

$$N_1(2k, t) = \begin{cases} q^{2k-1} + q^{k-1}(q-1) & \text{if} \quad t = 0, \\ q^{2k-1} - q^{k-1} & \text{if} \quad t \neq 0. \end{cases} \tag{2.7}$$

If $s = 2k+2$, then from (1.4),

$$Q_0(\xi) = \sum_{i=1}^{k} b_i b_{k+i} + b_{2k+1}^2 + b_{2k+1} b_{2k+2} + \beta b_{2k+2}^2$$

and (2.1) becomes

$$\begin{aligned} &qN_1(2k+2, t) \\ &= \sum_{c} e(ct) \sum_{b_{2k+1}} \sum_{b_{2k+2}} e(cb_{2k+1}^2 + cb_{2k+1} b_{2k+2} + c\beta b_{2k+2}^2) \prod_{i=1}^{k} \sum_{b_i} \sum_{b_{k+i}} e(cb_i b_{k+i}) \\ &= q^{2k+2} + \sum_{c\neq 0} e(ct) \sum_{y_1} \sum_{y_2} e(y_1^2 + y_1 y_2 + \beta y_2^2) \prod_{i=1}^{k} \sum_{b_i} \sum_{b_{k+i}} e(cb_i b_{k+i}) \\ &= q^{2k+2} + q^k \sum_{c\neq 0} e(ct) \sum_{y_1} \sum_{y_2} e(y_1^2 + y_1 y_2 + \beta y_2^2), \end{aligned} \tag{2.8}$$

where $y_1 = ab_{2k+1}$ and $y_2 = ab_{2k+2}$ with $a^2 = c$. Now Carlitz [1] has shown that

$$\sum_{y_1} \sum_{y_2} e(y_1^2 + y_1 y_2 + \beta y_2^2) = -q. \tag{2.9}$$

Hence,

$$N_1(2k+2, t) = \begin{cases} q^{2k+1} - (q-1)q^k & \text{if} \quad t = 0, \\ q^{2k-1} + q^k & \text{if} \quad t \neq 0. \end{cases} \tag{2.10}$$

3. Determination of $N(s; t, u, v)$. Let $\xi = (b_1, \ldots, b_s)$ be any of the $N_1(s; t)$ solutions to $Q_0(\xi) = t$, where $N_1(s; t)$ is given by one of (2.4), (2.7), or (2.10). Then $g_0(\xi, \chi)$ of (1.13) is given by one of the equations (1.5), (1.6), or (1.7) and may be denoted by $L_0(\chi)$, since it is for given ξ a linear function of $\chi = (x_1, \ldots, x_s)$. Thus, let $N_2(s; u, v)$ denote the number of solutions $\chi = (x_1, x_2, \ldots, x_s)$ to the simultaneous system of equations

$$Q_0(\chi) = u, \tag{3.1}$$

$$L_0(\chi) = v, \tag{3.2}$$

where $\xi = (b_1, \ldots, b_s)$ is any solution to $Q_0(\xi) = t$.

If for $s = 2k+1$, $\xi = (0, 0, \ldots, 0, \sqrt{t})$, then L_0 is the zero linear function and $N_1(s; u)$ of (2.4) gives the number of solutions χ to the system defined by (3.1) and (3.2) for $v = 0$. There are no solutions in this case if $v \neq 0$.

Also, if for any s, $\xi = (0, 0, \ldots, 0)$ is the specified solution to $Q_0(\xi) = 0$, L_0 is the zero linear function, and $N_1(s; u)$ of (2.4), (2.7), or (2.10) gives the number solutions χ to the system defined by (3.1) and (3.2) for $v = 0$ according as $s = 2k+1$, $2k$, or $2k+2$, respectively. There are no solutions in this case if $v \neq 0$.

Only if $\xi = (0, 0, \ldots, \sqrt{t})$ for $s = 2k+1$ or if $\xi = (0, 0, \ldots, 0)$ for any s, is L_0 the zero linear map. Thus, it will be implicit from the following arguments that

$$N(s; t, u, v) = \begin{cases} \big(N_1(s; t) - 1\big) N_2(s; u, v) + N_1(s; u) & \text{if } t = v = 0 \\ \quad \text{and } s \text{ is even or if } v = 0 \text{ and } s \text{ is odd}, \\ \big(N_1(s; t) - 1\big) N_2(s; u, v), & \text{if } t = 0,\ v \neq 0 \\ \quad \text{and } s \text{ is even or if } v \neq 0 \text{ and } s \text{ is odd}, \\ N_1(s; t) N_2(s; u, v), & \text{otherwise}. \end{cases} \tag{3.3}$$

Thus, let $\xi = (b_1, b_2, \ldots, b_s)$ be any of the solutions to $Q_0(\xi) = t$ such that L_0 is not the zero linear function. Hence, for each u in F, there exist q^{s-1} vectors $\chi = (x_1, x_2, \ldots, x_s)$ such that $L_0(\chi) = u$.

From (1.1), we obtain

$$\begin{aligned} q^2 N_2(s; u, v) &= \sum_{c} \sum_{d} \sum_{\chi} e\{c(Q_0(\chi) + u) + d(L_0(\chi) + v)\} \\ &= \sum_{c} \sum_{d} e(cu + dv) \sum_{\chi} e\{cQ_0(\chi) + dL_0(\chi)\} \\ &= q^s + \sum_{c\neq 0} \sum_{d} e(cu + dv) \sum_{\chi} e\{cQ_0(\chi) + dL_0(\chi)\}. \end{aligned} \tag{3.4}$$

Carlitz [2] has defined

$$G(Q, L) = \sum_{\chi} e\{Q(\chi)+L(\chi)\}. \tag{3.5}$$

Using (3.5) in (3.4), we have

$$q^2 N_2(s; u, v) = q^s + \sum_{c\neq 0}\sum_{d} e(cu+dv) G(cQ_0, dL_0). \tag{3.6}$$

If s is even, it can be determined from Carlitz work [1], [2] that

$$G(cQ_0, dL_0) = \tau q^{s/2} e(c^{-1}d^2 t) \quad \text{if} \quad c \neq 0, \tag{3.7}$$

where τ is the type of Q_0. Hence, for s even, (3.7) applied to (3.6) becomes

$$q^2 N_2(s; u, v) = q^s + \tau q^{s/2} \sum_{c\neq 0}\sum_{d} e(cu+dv) e(c^{-1}d^2 t). \tag{3.8}$$

If $t = 0$, then (3.8) becomes

$$q^2 N_2(s; u, v) = q^s + \tau q^{s/2} \sum_{c\neq 0} e(cu) \sum_{d} dv, \tag{3.9}$$

and (1.1) can be applied. Otherwise, if $t \neq 0$, then (3.8) becomes

$$q^2 N_2(s; u, v) = q^s + \tau q^{s/2} \sum_{c\neq 0} e(cu) \sum_{d} e(c^{-1}td^2 + vd). \tag{3.10}$$

In the latter sum in (3.10), let $r^2 = c^{-1}td^2$ and $k = \sqrt{ct^{-1}}$. Carlitz [1] has shown that

$$\sum_{r} (r^2 + ar) = \begin{cases} q & \text{if} \quad a = 1, \\ 0 & \text{if} \quad a \neq 1. \end{cases} \tag{3.11}$$

Therefore,

$$\sum_{d} e(c^{-1}td^2 + vd) = \sum_{r} e(r^2 + kvr) = \begin{cases} q & \text{if} \quad c = tv^{-2} \text{ with } v \neq 0, \\ 0 & \text{if} \quad v = 0 \text{ or if } c \neq tv^{-2} \text{ with } v \neq 0. \end{cases} \tag{3.12}$$

Hence,

(3.13)

$$N_2(s; u, v) = \begin{cases} q^{s-2} + \tau q^{(s-2)/2}(q-1), & t = u = v = 0, \\ q^{s-2} - \tau q^{(s-2)/2}, & t = v = 0, \ u \neq 0, \\ q^{s-2}, & t = 0, \ v \neq 0 \text{ or } t \neq 0, \ v = 0, \\ q^{s-2} + \tau q^{(s-2)/2} e(uv^{-2}t), & t \neq 0, \ v \neq 0, \qquad (s \text{ even}). \end{cases}$$

If s is odd, it can be determined from Carlitz work [1], [2] that

$$G(cQ_0, dL_0) = \begin{cases} q^{(s+1)/2} e(t + cd^{-2}) & \text{if} \quad c^{-1}d^2(b_s^*)^2 = 1, \\ 0 & \text{if} \quad c^{-1}d^2(b_s^*)^2 \neq 1, \end{cases} \tag{3.14}$$

where in Carlitz work $Q_0(\chi)$ is given by our equation (1.2) but where $L_0(\chi)$ is given by

$$L_0(\chi) = b_1^* x_{k+1} + \ldots + b_k^* x_{2k} + b_{k+1}^* x_1 + \ldots + b_{2k}^* x_k + b_{2k+1}^* x_{2k+1}.$$

However, in view of (1.5), the coefficient of x_{2k+1} in (3.2) is zero. Hence, for our purposes (3.14) reduces to

$$G(cQ_0, dL_0) = 0. \tag{3.15}$$

Applying (3.15) to (3.6), we obtain

$$N_2(s; u, v) = q^{s-2}, \quad s \text{ odd}. \tag{3.16}$$

Thus, by using (2.4), (2.7), or (2.10) for $N_1(s; t)$ and (3.13) or (3.16) for $N_2(s; u, v)$ in (3.3), we obtain $N(s; t, u, v)$.

4. An example. In determining [4] the number of $n\times s$ matrices X of rank r over $F = \mathrm{GF}(2^y)$ such that $XAX^T \equiv B \bmod \mathscr{A}_n$, the additive group of $n\times n$ alternate matrices, for given A and B, upper triangular matrices of full rank quadratic forms Q_1 and Q_2 on $F^{1\times s}$ and $F^{1\times n}$, respectively, we needed to determine $N(s; 1, \alpha, 1)$, the number of solutions $\begin{bmatrix}\xi\\ \chi\end{bmatrix}$ to the matrix equation

$$\begin{bmatrix}\xi\\ \chi\end{bmatrix} G_0[\xi^T, \chi^T] \equiv \begin{bmatrix}1 & 1\\ 0 & \alpha\end{bmatrix} \bmod \mathscr{A}_2, \tag{4.1}$$

where G_0 is the matrix of quadratic form Q_0 on $F^{1\times s}$ given by one of (1.2), (1.3), and (1.4) and where α is such that the polynomial $u^2 + uv + \alpha v^2$ is irreducible in $F[u, v]$.

Thus, the number solutions $N_1(s; 1)$ to $Q_0(\xi) = 1$ from (2.4), (2.7), and (2.10) is

$$N_1(s; 1) = \begin{cases} q^{s-1} & \text{if} \quad s \text{ is odd}, \\ q^{s-1} - \tau q^{(s-2)/2} & \text{if} \quad s \text{ is even}. \end{cases} \tag{4.2}$$

Let $\xi = (b_1, b_2, \ldots, b_s)$ be any solution to $Q_0(\xi) = 1$. If s is odd, the solution $\xi = (0, 0, \ldots, 0, 1)$ to $Q_0(\xi) = 1$ leads to L_0 being the zero linear function, and since $L_0(\chi) = g_0(\xi, \chi)$ must be 1, there are no solutions χ for this ξ to the system $g_0(\xi, \chi) = L_0(\chi) = 1$ and $Q_0(\chi) = \alpha$. Hence, if $\xi \neq (0, 0, \ldots, 0, 1)$ is a solution to $Q_0(\xi) = 1$, from (3.13) and (3.16) we find that

$$(4.3)\qquad N_2(s; a, 1) = \begin{cases} q^{s-2}, & s \text{ odd}, \\ q^{s-2} + \tau q^{(s-2)/2} e(a) = q^{s-2} - \tau q^{(s-2)/2}, & s \text{ even}, \end{cases}$$

where $e(a) = -1$ ([3], p. 199). Therefore, from (3.3), we obtain

$$(4.4)\qquad N(s; 1, a, 1) = \begin{cases} (q^{s-1} - 1) q^{s-2}, & s \text{ odd}, \\ (q^{s-1} - \tau q^{(s-2)/2})(q^{s-2} - \tau q^{(s-2)/2}), & s \text{ even}, \end{cases}$$

which is the number of solutions to (4.1).

References

[1] L. Carlitz, *Gauss sums over finite fields of order* 2^n, Acta Arith. 15 (1969), pp. 247–265.

[2] — *Reduction formulas for certain multiple exponential sums*, Czechoslovak Math. J. 20 (95) (1970), pp. 616–627.

[3] L. E. Dickson, *Linear groups with an exposition of the Galois theory*, New York 1958.

[4] J. D. Fulton, *Representations by quadratic forms in a finite field of characteristic two*, Math. Nachr. 77 (1977), pp. 237–243.

Received on 2. 9. 1976 (874)

ACTA ARITHMETICA
XXXV (1979)

Some results on p-extensions of local and global fields

by

ROBERT J. BOND (Chestnut Hill, Mass.)

1. Introduction. Let K be a local or a global field, p a prime, and $\tilde{K}$ the maximal p-extension of K; i.e., $\tilde{K}$ is the compositum of all Galois extensions of K of p-power degree. Let $G_K(p)$ be the Galois group of $\tilde{K}$ over K. The structure of $G_K(p)$ is well-known in the local case and is studied in some detail in the global case by Koch [3] and Höchsmann [2].

In this paper we consider the following question: what information about K is contained in $G_K(p)$ considered as an abstract pro-p-group? A similar question was answered by Neukirch in the case where K is a finite normal extension of the rationals. He shows in [4] that K is determined completely by the Galois group of the maximal solvable extensions of K over K. If K is a global field of non-zero characteristic, the effect of the Galois group of the separable closure of K over K is considered in [1].

Let K be a local field with residue class field k of characteristic $p_0 \neq p$. We prove that $G_K(p)$ determines $k^*(p)$, the p-primary part of the multiplicative group $k^* = k - \{0\}$. In the global case we show that $G_K(p)$ determines whether or not K has a primitive pth root of unity. We then restrict our attention to function fields with finite constant field k and show that $G_K(p)$ determines $k^*(p)$, $p \neq \operatorname{char} K$; more explicitly, if K and K' are two function fields of char $p_0 \neq p$ with constant fields k and k' respectively and if $G_K(p)$ and $G_{K'}(p)$ are isomorphic algebraically and topologically as pro-p-groups, then $k^*(p) \approx k'^*(p)$.

We then consider continuous automorphisms of $G_K(p)$ where K is a function field containing a primitive pth root of unity. We prove that if L is a constant field extensions of K of p-power degree, then $G_L(p)$ is a characteristic subgroup of $G_K(p)$.

First some notation. If K is a field, $\tilde{K}$ will denote the maximal p-extension of K and $G_K(p)$ or $G(\tilde{K}/K)$ the Galois group of $\tilde{K}$ over K. G_K will denote the Galois group of the separable closure of K over K. $H^n(G_K(p))$ will be the nth cohomology group $H^n(G_K(p), Z/pZ)$. If v is a valuation of K we let K_v be the completion of K with respect to v. We will write $\delta(K) = 1$ or 0 depending on whether or not K has a primitive pth root of unity.