d'un nombre fini des cas, aient un facteur premier idéal de degré 1 *dans J, il faut et il suffit que*

$$G(x) = aN(H(x)),$$

où $H(x)$ est un polynôme à coefficients de J, N est la norme dans J et a est un nombre rationnel.

La propriété des corps Baueriens exprimée dans ce théorème est caracteristique: pour les autres corps p.ex. $Q(\sqrt{2\cos(2\pi/7)})$ (cf. [4], p. 335) le théorème est en défaut.

Travaux cités

[1] M. Bauer, *Zur Theorie der algebraischen Zahlkörper*, Math. Ann. 77 (1916), p. 353-356.

[2] H. Davenport, D. J. Lewis and A. Schinzel, *Polynomials of certain special types*, Acta Arith. 9 (1964), p. 107-116.

[3] T. Nagell, *Sur les diviseurs premiers des polynômes*, Acta Arith. ce fasc., p. 235-244.

[4] A. Schinzel, *On a theorem of Bauer and some of its applications*, Acta Arith. 11 (1966), p. 333-344. Corrigendum, ibid. 12 (1967), p. 425.

Reçu par la Rédaction le 22. 6. 1968

ACTA ARITHMETICA
XV (1969)

Gauss sums over finite fields of order 2^n *

by

L. Carlitz (Durham, North Carolina)

1. Introduction. Let $F = \mathrm{GF}(q)$ denote the finite field of order q; we shall assume throughout the paper that $q = 2^n$, $n \geqslant 1$. For $a \in F$ put

$$t(a) = a + a^2 + a^{2^2} + \ldots + a^{2^{n-1}},$$

so that $t(a) \in \mathrm{GF}(2)$. Define

$$e(a) = (-1)^{t(a)}.$$

Let

$$Q(x) = Q(x_1, \ldots, x_m) = \sum_{1 \leqslant i \leqslant j \leqslant m} a_{ij} x_i x_j \quad (a_{ij} \in F) \tag{1.1}$$

denote a quadratic form over F. If

$$y_i = \sum_{j=1}^{m} c_{ij} x_j \quad (c_{ij} \in F, \ |c_{ij}| \neq 0)$$

and

$$Q(x_1, \ldots, x_m) = Q_1(y_1, \ldots, y_m),$$

the quadratic forms $Q(x)$ and $Q_1(y)$ are *equivalent*. Dickson ([2], p. 197) has proved that if $Q(x)$ is not equivalent to a form in fewer than m indeterminates then it is equivalent to either

$$y_1 y_2 + y_3 y_4 + \ldots + y_{m-2} y_{m-1} + y_m^2 \tag{1.2}$$

when m is odd or to one of the forms

$$y_1 y_2 + y_3 y_4 + \ldots + y_{m-1} y_m \tag{1.3}$$

or

$$y_1 y_2 + \ldots + y_{m-3} y_{m-2} + y_{m-1}^2 + y_{m-1} y_m + \beta y_m^2 \tag{1.4}$$

* Supported in part by NSF grant GP-1855.

when m is even. In the latter case β is any number of F such that the polynomial

$$u^2+uv+\beta v^2$$

is irreducible over $F[u, v]$. We shall say that $Q(x)$ is of *type* $\tau = +1$ or -1 according as it is equivalent to (1.3) or (1.4). We remark that $\tau = e(\beta)$.

We now define the sum

$$S(Q) = \sum_{c_1,\ldots,c_m \in F} e\big(Q(c_1, \ldots, c_m)\big). \tag{1.5}$$

However in the present situation it is of interest to consider a more general sum

$$S(Q, L) = \sum_{c_1,\ldots,c_m \in F} e\{Q(c_1, \ldots, c_m)+L(c_1, \ldots, c_m)\}, \tag{1.6}$$

where

$$L(x) = L(x_1, \ldots, x_m) = \sum_{j=1}^{m} b_j x_j \qquad (b_j \in F),$$

is an arbitrary linear form over F. For odd q there is no gain in generality in considering sums like (1.6); however, as we shall see, for even q, (1.6) is indeed more general than (1.5).

It is convenient to first treat the sum $S(Q)$. We assume that $Q(x)$ is not equivalent to a quadratic form in fewer than m indeterminates. Then we show that

$$S(Q) = 0 \qquad (m \text{ odd}), \tag{1.7}$$

$$S(Q) = \tau q^{m/2} \qquad (m \text{ even}), \tag{1.8}$$

where τ denotes the type of Q. The corresponding results for $S(Q, L)$ require some preliminaries and are contained in Theorems 6 and 7 below. It is not difficult to obtain these results when $Q(x)$ is assumed to be in one of the *normal* forms (1.2), (1.3) or (1.4). To state the results for arbitrary $Q(x)$ it is necessary to define first an invariant $\delta(Q)$ when m is even and an invariant $\eta(Q)$ when m is odd. In addition certain simultaneous invariants $\zeta(Q, L)$, $\omega(Q, L)$ for m even and odd, respectively, are also needed. For the first three invariants see Theorems 1 and 2 below, for $\omega(Q, L)$ see (4.15). These invariants suggest certain geometric questions that we hope to discuss elsewhere.

As an application we determine the number of solutions in F of the equation

$$Q(x)+L(x) = a. \tag{1.9}$$

More generally we show that the weighted sum

$$\sum_{c_1,\ldots,c_m} e(\lambda_1 c_1+\ldots+\lambda_m c_m) \qquad (\lambda_j \in F), \tag{1.10}$$

where the summation is over all solutions of (1.9), can be expressed in terms of the Kloosterman sum

$$K(a, b) = \sum_{c\neq 0} e(ac+bc^{-1}).$$

2. Preliminaries on quadratic forms. If $Q(x_1, \ldots, x_m)$ is equivalent to a form in r indeterminates but not in fewer than r, then Q is of *rank* r; if $r = m$, Q is *nonsingular*.

Let

$$Q(x) = \sum_{1\leqslant i\leqslant j\leqslant m} a_{ij} x_i x_j. \tag{2.1}$$

Put

$$\bar{a}_{ij} = \begin{cases} a_{ij} & (i<j), \\ a_{ji} & (i>j), \\ 0 & (i=j), \end{cases} \tag{2.2}$$

$$\delta = \delta(Q) = \det(\bar{a}_{ij}). \tag{2.3}$$

If

$$y_i = \sum_{j=1}^{m} c_{ij} x_j \qquad (i = 1, 2, \ldots, m), \tag{2.4}$$

where

$$c = \det(c_{ij}) \neq 0$$

and

$$Q(x) = Q_1(y) = \sum_{1\leqslant i\leqslant j} b_{ij} y_i y_j,$$

then

$$\frac{\partial Q(x)}{\partial x_i} = \sum_{s=1}^{m} \frac{\partial Q_1(y)}{\partial y_s} c_{si},$$

$$\frac{\partial^2 Q(x)}{\partial x_i \partial x_j} = \sum_{s,t=1}^{m} \frac{\partial^2 Q(y)}{\partial y_s \partial y_t} c_{si} c_{tj}. \tag{2.5}$$

On the other hand

$$\frac{\partial Q(x)}{\partial x_i} = \sum_{j=1}^{m} \bar{a}_{ij} x_j, \qquad \frac{\partial^2 Q(x)}{\partial x_i \partial x_j} = \bar{a}_{ij},$$

so that (2.4) reduces to

$$a_{ij} = \sum_{s,t=1}^{m} \bar{b}_{st} c_{si} c_{tj},$$

where

$$\bar{b}_{st} = \begin{cases} b_{st} & (s < t), \\ b_{ts} & (s > t), \\ 0 & (s = t). \end{cases}$$

It therefore follows at once that

$$\delta(Q) = c^2 \delta(Q_1), \tag{2.6}$$

that is to say, δ is a relative invariant of weight two.

If m is odd it is easily seen that $\delta(Q)$ vanishes identically. For m even, however, if

$$Q(x) = x_1 x_2 + x_3 x_4 + \ldots + x_{m-1} x_m$$

then it can be verified that $\delta(Q) = 1$.

When m is odd we shall construct an invariant that does not vanish identically in the following way.

Some preliminaries are needed. If B is a skew matrix of even order:

$$B = (b_{ij}) \qquad (b_{ij} = b_{ji},\ b_{ii} = 0),$$

it is readily seen that $\det B$ is equal to the square of a polynomial in the b_{ij}. Indeed this can be stated quite explicitly. We have for example

$$\begin{vmatrix} \cdot & b_{12} \\ b_{21} & \cdot \end{vmatrix} = b_{12}^2,$$

$$\begin{vmatrix} \cdot & b_{12} & b_{13} & b_{14} \\ b_{21} & \cdot & b_{23} & b_{24} \\ b_{31} & b_{32} & \cdot & b_{34} \\ b_{41} & b_{42} & b_{43} & \cdot \end{vmatrix} = (b_{12}b_{34} + b_{13}b_{14} + b_{14}b_{23})^2,$$

$$\begin{vmatrix} \cdot & b_{12} & b_{13} & b_{14} & b_{15} & b_{16} \\ b_{21} & \cdot & b_{23} & b_{24} & b_{25} & b_{26} \\ b_{31} & b_{32} & \cdot & b_{34} & b_{35} & b_{36} \\ b_{41} & b_{42} & b_{43} & \cdot & b_{45} & b_{46} \\ b_{51} & b_{52} & b_{53} & b_{54} & \cdot & b_{56} \\ b_{61} & b_{62} & b_{63} & b_{64} & b_{65} & \cdot \end{vmatrix} = \begin{aligned}(&b_{12}b_{34}b_{56} + b_{13}b_{24}b_{56} + b_{14}b_{23}b_{56} + \\ &+ b_{12}b_{35}b_{46} + b_{13}b_{25}b_{46} + b_{15}b_{23}b_{46} + \\ &+ b_{12}b_{45}b_{36} + b_{14}b_{25}b_{36} + b_{15}b_{24}b_{36} + \\ &+ b_{13}b_{45}b_{26} + b_{14}b_{35}b_{26} + b_{15}b_{34}b_{26} + \\ &+ b_{23}b_{45}b_{16} + b_{24}b_{35}b_{16} + b_{25}b_{34}b_{16})^2.\end{aligned}$$

The general expression for $\det B$ can now be written down without any difficulty. Incidentally the number of terms is equal to $(2s)!/(2!)^s s!$, where B is of order $2s$.

With $\bar{a}_{ij}$ defined by (2.2) put

$$\bar{Q}(u) = \begin{vmatrix} \cdot & \bar{a}_{12} & \bar{a}_{13} & \ldots & \bar{a}_{1m} & u_1 \\ \bar{a}_{21} & \cdot & \bar{a}_{23} & \ldots & \bar{a}_{2m} & u_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \bar{a}_{m1} & \bar{a}_{m2} & \ldots & & \cdot & u_m \\ u_1 & u_2 & \ldots & & u_m & \cdot \end{vmatrix}. \tag{2.7}$$

For m even, $\bar{Q}(u)$ vanishes identically. For m odd, on the other hand, it is clear from the above that

$$\bar{Q}(u) = \left(\sum_{j=1}^{m} A_j u_j\right)^2, \tag{2.8}$$

where the A_j are certain well-defined polynomials in $\bar{a}_{ik}$. For example, for $m = 3$ we have

$$\bar{Q}(u) = (a_{23}u_1 + a_{13}u_2 + a_{12}u_3)^2,$$

while for $m = 5$

$$\begin{aligned}\bar{Q}(u) = \ &\{(a_{23}a_{45} + a_{24}a_{35} + a_{25}a_{34})u_1 + \\ &+ (a_{13}a_{45} + a_{14}a_{35} + a_{15}a_{34})u_2 + \\ &+ (a_{12}a_{45} + a_{14}a_{25} + a_{15}a_{24})u_3 + \\ &+ (a_{12}a_{35} + a_{13}a_{25} + a_{15}a_{23})u_4 + \\ &+ (a_{12}a_{34} + a_{13}a_{24} + a_{14}a_{23})u_5\}^2.\end{aligned}$$

Again the mode of formation of the coefficients is clear.

We now define

$$\eta(Q) = Q(A_1, A_2, \ldots, A_m), \tag{2.9}$$

where $Q(x)$ is an arbitrary quadratic form with m odd. For example when $m = 3$ we have

$$\eta(Q) = a_{11}a_{23}^2 + a_{22}a_{13}^2 + a_{33}a_{12}^2 + a_{12}a_{13}a_{23}.$$

For

$$Q_0 = x_1x_2 + \ldots + x_{m-2}x_{m-1} + x_m^2 \tag{2.10}$$

we find that

$$A_1 = \ldots = A_{m-1} = 0, \qquad A_m = 1$$

and therefore

$$\eta(Q_0) = 1. \tag{2.11}$$

Thus $\eta(Q)$ does not vanish identically.

To see how $\eta(Q)$ transforms when $Q(x)$ is subjected to a nonsingular linear transformation we assume that the u_j in (2.7) transform contragriently to the x_i. For brevity we replace (2.7) by

$$\bar{Q}(u) = \begin{vmatrix} \bar{A} & u \\ u' & \cdot \end{vmatrix}, \tag{2.12}$$

where $\bar{A} = (\bar{a}_{ij})$, u is the column vector $(u_1, \ldots, u_m)$ and u' is the corresponding row vector; similarly x is the column vector $(x_1, \ldots, x_m)$ and y the column vector $(y_1, \ldots, y_m)$. Thus (2.4) becomes $y = Cx$, where $C = (c_{ij})$, while

$$C'v = u, \tag{2.13}$$

where C' is the transpose of C and $v = \operatorname{col}(v_1, \ldots, v_m)$. Since

$$\bar{A} = C'\bar{B}C,$$

where $\bar{B} = (\bar{b}_{ij})$, it follows from (2.12) that

$$Q(u) = \begin{vmatrix} C'BC & C'v \\ v'C & . \end{vmatrix}.$$

Therefore

$$\bar{Q}(u) = c^2\bar{Q}_1(v), \tag{2.14}$$

where

$$\bar{Q}_1(v) = \begin{vmatrix} \bar{B} & v \\ v' & . \end{vmatrix} = \sum_{i=1}^{m} B_i v_i .$$

Hence by (2.8) and (2.14)

$$\sum_{i=1}^{m} A_i u_i = c \sum_{i=1}^{m} B_i v_i ,$$

which, in view of (2.13) implies

$$cB_i = \sum_{j=1}^{m} c_{ij} A_j \qquad (i = 1, 2, \ldots, m). \tag{2.15}$$

Now applying (2.9) we get

$$\eta(Q) = c^2 \eta(Q_1), \tag{2.16}$$

so that $\eta(Q)$ is a relative invariant of weight two.

We shall also require, when m is even, a simultaneous invariant of the pair of forms $Q(x)$, $L(x)$, where

$$L(x) = \sum_{i=1}^{m} a_i x_i .$$

Put

$$Q_i(x) = \frac{\partial Q(x)}{\partial x_i} = \sum_{j=1}^{m} \bar{a}_{ij} x_j .$$

We assume that $\delta(Q) \neq 0$, so that the system of equations

$$Q_i(x) = a_i \qquad (i = 1, 2, \ldots, m) \tag{2.17}$$

has the unique solution $(a_1^*, a_2^*, \ldots, a_m^*)$. Now define

$$\zeta(Q, L) = Q(a_1^*, a_2^*, \ldots, a_m^*). \tag{2.18}$$

Applying the transformation (2.4), assume that $L(x)$ becomes

$$L_1(y) = \sum_{i=1}^{m} b_i y_i$$

and let the system

$$\frac{\partial Q_1(x)}{\partial x_i} = b_i \qquad (i = 1, 2, \ldots, m)$$

have the unique solution $(b_1^*, b_2^*, \ldots, b_m^*)$. Let a, b denote the column vectors $(a_1, a_2, \ldots, a_m), (b_1, b_2, \ldots, b_m)$ and similarly for a^*, b^*. Then we have

$$\bar{A}a^* = a, \qquad \bar{B}b^* = b; \tag{2.19}$$

moreover we have

$$a = C'b. \tag{2.20}$$

It now follows easily from (2.19) and (2.20) that

$$b^* = Ca^*, \tag{2.21}$$

so that the a_i^* transform exactly like the x_i. Consequently (2.18) yields

$$\zeta(Q, L) = \zeta(Q_1, L_1). \tag{2.22}$$

Thus $\zeta(Q, L)$ is an absolute invariant.

The results of this section may be summarized in the following two theorems.

THEOREM 1. *For m even, $\delta(Q)$ is a relative invariant of weight two. For m odd, $\eta(Q)$ is a relative invariant of weight two.*

THEOREM 2. *For m even and $\delta(Q) \neq 0$, $\zeta(Q, L)$ is a simultaneous absolute invariant.*

We note that if

$$Q_0(x) = x_1x_2 + x_3x_4 + \ldots + x_{m-1}x_m$$

then

$$\zeta(Q_0, L) = a_1a_2 + a_3a_4 + \ldots + a_{m-1}a_m \tag{2.23}$$

but if

$$Q_0(x) = x_1x_2 + \ldots + x_{m-3}x_{m-2} + x_{m-1}^2 + x_{m-1}x_m + \beta x_m^2$$

then

$$\zeta(Q_0, L) = a_1a_2 + \ldots + a_{m-1}a_{m-2} + a_m^2 + a_m a_{m-1} + \beta a_{m-1}^2. \tag{2.24}$$

Remark. For m even, $Q(x)$ is nonsingular if and only if $\delta(Q) \neq 0$; for m odd, $Q(x)$ is nonsingular if and only if $\eta(Q) \neq 0$.

3. Evaluation of $S(Q)$. We shall make frequent use of the formula

$$\sum_{\beta} e(a\beta) = \begin{cases} q & (a = 0), \\ 0 & (a \neq 0), \end{cases} \tag{3.1}$$

where the summation is over all $\beta \in F$. In what follows we shall usually indicate summations in this way.

It follows at once from the definition

$$S(Q) = \sum_{c_1, \ldots, c_m} e\big(Q(c_1, \ldots, c_m)\big)$$

that if Q_1 is equivalent to Q then

$$S(Q_1) = S(Q). \tag{3.2}$$

However, as we shall see, the converse is in general not true.

In view of (3.2) we may assume that Q is in normal form. We assume Q nonsingular. Hence we may put

$$Q = x_1x_2 + \ldots + x_{m-2}x_{m-1} + x_m^2 \quad (m \text{ odd}) \tag{3.3}$$

or, when m is even,

$$Q = \begin{cases} x_1x_2 + \ldots + x_{m-3}x_{m-2} + x_{m-1}x_m, \\ x_1x_2 + \ldots + x_{m-3}x_{m-2} + x_{m-1}^2 + x_{m-1}x_m + \beta x_m^2 \end{cases} \tag{3.4}$$

according as Q is of type $+1$ or -1.

Since by (3.1)

$$\sum_a e(a^2) = 0,$$

it follows at once from (3.3) that

$$S(Q) = 0 \quad (m \text{ odd}).$$

In the next place, by (3.1),

$$\sum_{a,b} e(ab) = q. \tag{3.5}$$

Hence for Q of type $+1$ we have

$$S(Q) = q^{m/2} \quad (\tau = +1). \tag{3.6}$$

For Q of type -1 we have

$$S(Q) = q^{(m-2)/2} \sum_{a,b} e(a^2 + ab + \beta b^2). \tag{3.7}$$

Now since $x^2 + xy + \beta y^2$ is irreducible in $F[x, y]$ it follows that the equation

$$x^2 + xy + \beta y^2 = 0$$

has the single solution $(0, 0)$. On the other hand the number of solutions of

$$x^2 + xy + \beta y^2 = a \quad (a \neq 0)$$

is independent of a and is therefore equal to $q+1$. It follows that

$$\sum_{a,b} e(a^2 + ab + \beta b^2) = 1 + (q+1) \sum_{a \neq 0} e(a) = -q. \tag{3.8}$$

Thus (3.7) becomes

$$S(Q) = -q^{m/2}. \tag{3.9}$$

We may now state

THEOREM 3. *Let*

$$Q(x) = \sum_{1 \leqslant i \leqslant j \leqslant m} a_{ij} x_i x_j \quad (a_{ij} \in F)$$

be a nonsingular quadratic form over F. Then

$$S(Q) = \begin{cases} 0 & (m \text{ odd}), \\ \tau q^{m/2} & (m \text{ even}), \end{cases} \tag{3.10}$$

where τ denotes the type of Q.

Suppose now that Q is of rank $r \leqslant m$. If r is odd it follows at once that $S(Q) = 0$. If r is even and Q is equivalent to $Q_0(x_1, \ldots, x_r)$ of type τ, then by (3.9)

$$S(Q) = \tau q^{r/2} q^{m-r} = \tau q^{(2m-r)/2}.$$

In particular this establishes the invariance of r and τ. Moreover if $Q_1(x_1, \ldots, x_m)$ also satisfies

$$S(Q_1) = \tau q^{(2m-r)/2}$$

it follows that Q and Q_1 are equivalent.

This proves

THEOREM 4. *The quadratic form $Q(x)$ is of odd rank if and only if $S(Q) = 0$. If*

$$S(Q) = \tau q^k \quad (m/2 \leqslant k \leqslant m)$$

then Q is of rank $r = 2(m-k)$ and type τ. Moreover two forms Q, Q_1 of even rank are equivalent if and only if $S(Q) = S(Q_1)$.

Thus for forms of even rank $S(Q)$ furnishes a criterion for equivalence. For odd rank however this is not the case.

The following corollary of Theorem 1 may be noted.

THEOREM 5. *If $Q_1(x_1, \ldots, x_{2s})$ is nonsingular of type τ_1 and $Q_2(y_1, \ldots \ldots, y_{2t})$ is nonsingular of type τ_2 then*

$$Q_1(x_1, \ldots, x_{2s})+Q_2(y_1, \ldots, y_{2t})$$

is nonsingular of type $\tau_1\tau_2$.

4. Evaluation of $S(Q, L)$. We shall require several preliminary results.

LEMMA 1.

$$\sum_{\lambda,\mu} e(\lambda\mu+a\lambda+b\mu) = qe(ab). \tag{4.1}$$

Proof. The sum is equal to

$$\sum_{\lambda,\mu} e\big((\lambda+b)(\mu+a)+ab\big) = e(ab)\sum_{\lambda,\mu} e(\lambda\mu)$$

and (4.1) follows at once.

LEMMA 2. *Let $x^2+xy+\beta y^2$ be irreducible over F. Then*

$$\sum_{\lambda,\mu} e(\lambda^2+\lambda\mu+\beta\mu^2+a\lambda+b\mu) = -qe(b^2+ab+\beta a^2). \tag{4.2}$$

Proof. Replacing λ, μ by $\lambda+b$, $\mu+a$, the sum becomes

$$\sum_{\lambda,\mu} e(\lambda^2+\lambda\mu+\beta\mu^2+b^2+ab+\beta a^2) = -qe(b^2+ab+\beta a^2)$$

by (3.8).

Define

$$R(a) = \sum_{\lambda} e(\lambda^2+a\lambda). \tag{4.3}$$

LEMMA 3.

$$R(a) = \begin{cases} q & (a=1), \\ 0 & (a\neq 1). \end{cases} \tag{4.4}$$

Proof. We have

$$R^2(a) = \sum_{\lambda,\mu} e[(\lambda+\mu)^2+a(\lambda+\mu)] = q\sum_{\lambda} e(\lambda^2+a\lambda),$$

so that

$$R^2(a) = qR(a). \tag{4.5}$$

Hence $R(a) = 0$ or q. On the other hand

$$\sum_a R(a) = \sum_a\sum_\lambda e(\lambda^2+a\lambda) = \sum_\lambda e(\lambda^2)\sum_a e(a\lambda).$$

By (3.1) this reduces to

$$\sum_a R(a) = q. \tag{4.6}$$

We now show that

$$R(1) = q. \tag{4.7}$$

Indeed

$$t(\lambda^2+\lambda) = \lambda^{2^n}+\lambda = 0, \quad e(\lambda^2+\lambda) = 1,$$

and (4.7) follows at once. Finally combining (4.5), (4.6) and (4.7) we get (4.4).

We now assume that $Q(x)$ is in normal form (3.3) or (3.4) and that

$$L(x) = a_1x_1+\ldots+a_mx_m. \tag{4.8}$$

If m is even and Q is of type $+1$, then it is evident that

$$S(Q, L) = \prod_{j=1}^{m/2}\sum_{\lambda,\mu} e(\lambda\mu+a_{2j-1}\lambda+a_{2j}\mu).$$

Applying Lemma 1 we get

$$S(Q, L) = q^{m/2}e(a_1a_2+\ldots+a_{m-1}a_m). \tag{4.9}$$

If m is even and Q is of type -1, then

$$S(Q, L) = \prod_{j=1}^{(m-2)/2}\sum_{\lambda,\mu} e(\lambda\mu+a_{2j-1}\lambda+a_{2j}\mu) = \sum_{\lambda,\mu} e(\lambda^2+\lambda\mu+\beta\mu^2+a_{m-1}\lambda+a_m\mu).$$

Applying Lemmas 1 and 2 we get

$$S(Q, L) = -q^{m/2}e(a_1a_2+\ldots+a_{m-3}a_{m-2}+a_m^2+a_ma_{m-1}+\beta a_{m-1}^2). \tag{4.10}$$

If m is odd we have

$$S(Q, L) = \prod_{j=1}^{(m-1)/2}\sum_{\lambda,\mu} e(\lambda\mu+a_{2j-1}\lambda+a_{2j}\mu)\sum_\lambda e(\lambda^2+a_m\lambda).$$

Applying Lemmas 1 and 3 we get

$$S(Q, L) = \begin{cases} q^{(m+1)/2}e(a_1a_2+\ldots+a_{m-2}a_{m-1}) & (a_m=1), \\ 0 & (a_m\neq 1). \end{cases} \tag{4.11}$$

By means of (4.9), (4.10) and (4.11) we have evaluated $S(Q, L)$ when Q is assumed to be in normal form. We shall now express these results in an invariantive form.

We first consider the case m even. Comparing (2.23) with (4.9) we get

$$S(Q,L) = q^{m/2}e[\zeta(Q,L)]$$

when Q is of type $+1$; comparing (2.24) with (4.10) we get

$$S(Q,L) = -q^{m/2}e[\zeta(Q,L)]$$

when Q is of type -1. We may therefore state

THEOREM 6. *If m is even and $Q(x)$ is nonsingular we have*

$$S(Q,L) = q^{m/2}\tau(Q)e[\zeta(Q,L)]. \tag{4.12}$$

When m is odd let

$$Q_0(x) = x_1x_2+\ldots+x_{m-2}x_{m-1}+x_m^2.$$

By (2.11) we have $\eta(Q_0)=1$. If the transformation

$$y_i = \sum_{j=1}^{m} c_{ij}x_j \qquad (i=1,2,\ldots,m)$$

carries $Q_0(x)$ into $Q(y)$, it follows from (2.15) that

$$c^2\eta(Q) = 1. \tag{4.13}$$

In the next place consider $Q(a_1,a_2,\ldots,a_m)$ as defined by (2.7). In particular by a simple calculation we get

$$\bar{Q}_0(a_1,a_2,\ldots,a_m) = a_m^2. \tag{4.14}$$

By (2.8) we have

$$\bar{Q}(a_1,a_2,\ldots,a_m) = \Big(\sum_{i=1}^{m} A_ia_i\Big)^2.$$

By (2.15) and (2.20)

$$\sum_{i=1}^{m} A_ia_i = c\sum_{i=1}^{m} B_ib_i.$$

It follows that

$$\omega(\bar{Q},L) = Q(a_1,a_2,\ldots,a_m)/\eta(Q) \tag{4.15}$$

is an absolute invariant which reduces to a_m^2 when $Q=Q_0$.

It remains to give an invariantive description of the coefficient

$$e(a_1a_2+\ldots+a_{m-2}a_{m-1})$$

occurring in the right member of (4.11). To do this we consider the quadratic form $Q(x)+tL(x)$ in the $m+1$ indeterminates $x_1,\ldots,x_m,t$. When $Q=Q_0$ we find that

$$\begin{aligned}Q_0(x)+tL(x) &= x_1x_2+\ldots+x_{m-2}x_{m-1}+x_m^2+t\sum_{i=1}^{m} a_ix_i\\ &= (x_1+a_2t)(x_2+a_1t)+\ldots+(x_{m-2}+a_{m-1}t)(x_{m-1}+a_{m-2}t)+\\ &\qquad +x_m^2+a_mx_mt+(a_1a_2+\ldots+a_{m-2}a_{m-1})t^2.\end{aligned}$$

We may assume that $a_m=1$. It follows that

$$\tau(Q_0+tL) = e(a_1a_2+\ldots+a_{m-2}a_{m-1}).$$

We may now state

THEOREM 7. *If m is odd and $Q(x)$ is nonsingular, then*

$$S(Q,L) = \begin{cases} q^{(m+1)/2}\tau(Q+tL) & (\omega(Q,L)=1),\\ 0 & (\omega(Q,L)\neq 1),\end{cases} \tag{4.16}$$

where $\omega(Q,L)$ is defined by (4.15).

5. Number of solutions. As an application of the results of § 4 we shall now determine the number of solutions of the equation

$$Q(x_1,\ldots,x_m)+L(x_1,\ldots,x_m) = a, \tag{5.1}$$

where $Q(x)$ is nonsingular and $L(x)$ is arbitrary. If we let N denote the number of solutions of (5.1) then by (3.1)

$$\begin{aligned}qN &= \sum_{c_1,\ldots,c_m}\sum_b e\{ab+bQ(c)+bL(c)\}\\ &= q^m+\sum_{b\neq 0}e(ab)\sum_{c_1,\ldots,c_m} e\{bQ(c)+bL(c)\}.\end{aligned}$$

Hence

$$N = q^{m-1}+q^{-1}\sum_{b\neq 0}e(ab)S(bQ,bL). \tag{5.2}$$

We consider first the case m even. It is clear from the definition of $\tau(Q)$ that

$$\tau(bQ) = \tau(Q) \qquad (b\neq 0). \tag{5.3}$$

Also it follows from the definition of $\zeta(Q,L)$ that

$$\zeta(bQ,bL) = b\zeta(Q,L) \qquad (b\neq 0). \tag{5.4}$$

Thus by (4.12), (5.3) and (5.4)

$$\sum_{b\neq 0}e(ab)S(bQ,bL) = q^{m/2}\tau(Q)\sum_{b\neq 0}e\big[\big(a+\zeta(Q,L)\big)b\big].$$

It is convenient to define

$$k(a) = \sum_{b\neq 0} e(ab) = \begin{cases} q-1 & (a=0), \\ -1 & (a\neq 0). \end{cases} \tag{5.5}$$

Then clearly

$$\sum_{b\neq} e(ab)S(bQ, bL) = q^{m/2}\tau(Q)k[a+\zeta(Q, L)]. \tag{5.6}$$

Substituting from (5.6) in (5.2) we obtain

THEOREM 8. *For m even and $Q(x)$ nonsingular the number of solutions of* (5.1) *is given by*

$$N = q^{m-1}+q^{(m-2)/2}\tau(Q)k[a+\zeta(Q, L)]. \tag{5.7}$$

Turning now to the case m odd it is clear from (5.3) that

$$\tau(bQ+btL) = \tau(Q+tL) \quad (b\neq 0).$$

Also it is evident from the definition that

$$\omega(bQ, bL) = b\omega(Q, L) \quad (b\neq 0).$$

Thus (4.16) gives

$$S(bQ, bL) = \begin{cases} q^{(m+1)/2}\tau(Q+tL) & (b\omega(Q, L)=1), \\ 0 & (b\omega(Q, L)\neq 1) \end{cases}$$

and therefore

$$\sum_{b\neq 0} e(ab)S(bQ, bL) = q^{(m+1)/2}\tau(Q+tL)e\{a/\omega(Q, L)\}.$$

Substituting in (5.2) we get

THEOREM 9. *For m odd and $Q(x)$ nonsingular the number of solutions of* (5.1) *is given by*

$$N = q^{m-1}+q^{(m-1)/2}\tau(Q+tL)e\{a/\omega(Q, L)\}, \tag{5.8}$$

provided $\omega(Q,L)\neq 0$. If however $\omega(Q,L)=0$ then we have

$$N = q^{m-1}. \tag{5.9}$$

It may be of interest to state these results when the linear form $L(x)$ is identically zero. We find that (5.7) reduces to

$$N = q^{m-1}+q^{(m-2)/2}\tau(Q) \quad (m \text{ even}). \tag{5.7'}$$

Since $\omega(Q, 0) = 0$, (5.8) does not apply and we have only

$$N = q^{m-1} \quad (m \text{ odd}). \tag{5.9'}$$

It is not difficult to prove (5.7)′ and (5.9)′ directly.

6. Weighted sums. Let $\lambda_1, \ldots, \lambda_m$ be arbitrary elements of $GF(q)$ and consider the sum

$$N(\lambda) = N(\lambda; Q, L) = \sum e(\lambda_1 c_1+\ldots+\lambda_m c_m), \tag{6.1}$$

where the summation is extended over all solutions of

$$Q(x_1, \ldots, x_m)+L(x_1, \ldots, x_m) = a. \tag{6.2}$$

As above we assume that $Q(x)$ is nonsingular while $L(x)$ is arbitrary. Clearly

$$qN(\lambda) = \sum_{c_1,\ldots,c_m}\sum_b e\{ab+bQ(c)+bL(c)+\Lambda(c)\}, \tag{6.3}$$

where for brevity we put

$$\Lambda(c) = \lambda_1 c_1+\ldots+\lambda_m c_m.$$

We rewrite (6.3) in the form

$$N(\lambda) = q^{-1}\sum_{c_1,\ldots,c_m} e(\Lambda(c))+q^{-1}\sum_{b\neq 0} e(ab)\sum_{c_1,\ldots,c_m} e\{bQ(c)+bL(c)+\Lambda(c)\}.$$

Put

$$A(\lambda) = \sum_{c_1,\ldots,c_m} e(\Lambda(c)) = \begin{cases} q^m & (\lambda_1 = \ldots = \lambda_m = 0), \\ 0 & (\text{otherwise}). \end{cases} \tag{6.4}$$

Then it is evident that

$$N(\lambda) = q^{-1}A(\lambda)+q^{-1}\sum_{b\neq 0} e(ab)S(bQ, bL+\Lambda). \tag{6.5}$$

For m even we have, by (5.3) and (5.4),

$$S(bQ, bL+\Lambda) = q^{m/2}\tau(Q)e[b\zeta(Q, L+b^{-1}\Lambda)].$$

To evaluate $\zeta(Q, L+b^{-1}\Lambda)$ let

$$\sum_{j=1}^m \bar{a}_{ij}c_j = a_i, \quad \sum_{j=1}^m \bar{a}_{ij}d_j = \lambda_i \quad (i = 1, 2, \ldots, m).$$

Then

$$\zeta(Q, L+b^{-1}\Lambda) = Q(c_1+b^{-1}d_1, \ldots, c_m+b^{-1}d_m) = \zeta(Q, L)+b^{-1}\lambda+b^{-2}\zeta(Q, \Lambda),$$

where

$$\xi = \sum_{i,j=1}^m b_{ij}a_i\lambda_j, \quad (\bar{a}_{ij})(b_{ij}) = I. \tag{6.6}$$

Hence

$$S(bQ, bL+A) = q^{m/2}\tau(Q)e\{b\zeta(Q, L)+\xi+b^{-1}\zeta(Q, A)\}$$

and (6.5) becomes

$$N(\lambda) = q^{-1}A(\lambda)+q^{(m-2)/2}\tau(Q)e(\xi)\sum_{b\neq 0} e\{ab+b\zeta(Q, L)+b^{-1}\zeta(Q, A)\}.$$

If we define the Kloosterman sum

(6.7) $$K(a, b) = \sum_{c\neq 0} e(ac+bc^{-1}),$$

then it is clear that

(6.8) $$N(\lambda) = q^{-1}A(\lambda)+q^{(m-2)/2}\tau(Q)e(\xi)K\{a+\zeta(Q, L), \zeta(Q, A)\}.$$

This proves

THEOREM 10. *For m even and $Q(x)$ nonsingular the sum $N(\lambda)$ satisfies* (6.8) *with $A(\lambda)$, ξ defined by* (6.4), (6.6), *respectively.*

For m odd we have by (4.16)

$$S(bQ, bL+A) = q^{(m+1)/2}\tau\{bQ+t(bL+A)\}$$

provided $\omega(bQ, bL+A) = 1$ and 0 otherwise. It is easily verified that

$$\omega(bQ, bL+A) = b\omega(Q, L)+b^{-1}\omega(Q, A).$$

The following theorem now follows at once.

THEOREM 11. *For m odd and $Q(x)$ nonsingular we have*

(6.9) $$N(\lambda) = q^{-1}A(\lambda)+q^{(m-1)/2}\sum_{b}{}'' e(ab)\tau\{bQ+t(bL+A)\},$$

where the summation on the right is over all b such that

(6.10) $$b\omega(Q, L)+b^{-1}\omega(Q, A) = 1.$$

Remark. Equation (6.10) has two solutions if

$$\omega(Q, L)\omega(Q, A)\neq 0, \quad e\{\omega(Q, L)\omega(Q, A)\} = 1;$$

one solution if just one of $\omega(Q, L)$, $\omega(Q, A) = 0$; otherwise there are no solutions.

For results corresponding to Theorems 10 and 11 when q is odd see [1].

7. Kloosterman sums. We conclude with a few properties of the sum

(7.1) $$K(a, b) = \sum_{c\neq 0} e(ac+bc^{-1}).$$

Clearly $K(a, b) = K(b, a)$ and

$$K(a, 0) = k(a),$$

with $k(a)$ defined by (5.5). Also it is evident that

(7.2) $$K(a, b) = K(ab, 1) \quad (ab\neq 0).$$

This implies

(7.3) $$K(a, b) = K(c, c) \quad (ab = c^2\neq 0).$$

It follows at once from (7.1) that $K(a, b)$ is an odd integer. Also since

$$\sum_{a} K(a, 1) = \sum_{b\neq 0} e(b^{-1})\sum_{a} e(ab) = 0,$$

we have

(7.4) $$\sum_{a\neq 0} K(a, 1) = 1.$$

Thus it is clear that, for $q>2$, $K(a, 1)$ takes on both positive and negative values.

Since

$$K(a^2, 1) = \sum_{b\neq 0} e(a^2b+b^{-1}) = \sum_{b\neq 0} e(a^2b^2+b^{-2}) = \sum_{b\neq 0} e(ab+b^{-1}),$$

it follows that

$$K(a, 1) = K(a^2, 1) = \ldots = K(a^{2^{n-1}}, 1).$$

If n is prime and $a\neq 1$, the numbers $a, a^2, \ldots, a^{2^{n-1}}$ are distinct. Hence (7.4) implies

(7.5) $$K(1, 1)\equiv 1 \pmod{n} \quad (n \text{ prime}).$$

In the next place

$$\sum_{a} K^2(a, 1) = \sum_{a}\sum_{b,c\neq 0} e\big(a(b+c)+b^{-1}+c^{-1}\big)$$
$$= \sum_{b,c\neq 0} e(b^{-1}+c^{-1})\sum_{a} e\big(a(b+c)\big) = q(q-1)$$

and therefore

(7.6) $$\sum_{a\neq 0} K^2(a, 1) = q^2-q-1.$$

To evaluate the sum of the cubes take

$$\sum_{a,b} K^3(a, b) = \sum_{a,b}\sum_{x,y,z\neq 0} e\{a(x+y+z)+b(x^{-1}+y^{-1}+z^{-1})\} = q^2N,$$

where N denotes the number of nonzero solutions of the system

$$x+y+z = 0,$$
$$\frac{1}{x}+\frac{1}{y}+\frac{1}{z} = 0.$$

This number is equal to the number of nonzero solutions of

$$x^2+xy+y^2 = 0.$$

For $q = 2^n$, n odd, x^2+xy+y^2 is irreducible in $F[x,y]$, so that $N = 0$. For n even, on the other hand, we have $N = 2(q-1)$. Thus

$$\sum_{a,b} K^3(a,b) = \begin{cases} 2q^2(q-1) & (n \text{ even}), \\ 0 & (n \text{ odd}). \end{cases}$$

Since $K(0,0) = q-1$ and

$$\sum_{a\neq 0} K^3(a,0) = \sum_{b\neq 0} K^3(0,b) = -(q-1),$$

it follows that

$$\sum_{a,b\neq 0} K^3(a,b) = \begin{cases} q^3+q^2-q-1 & (n \text{ even}), \\ -(q-1)^3+2(q-1) & (n \text{ odd}) \end{cases}$$

and therefore

(7.7) $$\sum_{a\neq 0} K^3(a,1) = \begin{cases} (q+1)^2 & (n \text{ even}), \\ -(q^2-2q-1) & (n \text{ odd}). \end{cases}$$

For the sum of the fourth powers we have

$$\sum_{a,b} K^4(a,b) = q^2 M,$$

where M is the number of nonzero solutions of

$$x+y+z+t = 0,$$
$$\frac{1}{x}+\frac{1}{y}+\frac{1}{z}+\frac{1}{t} = 0.$$

This system is equivalent to

$$(x+y)(x+z)(y+z) = 0,$$
$$xyz(x+y+z) \neq 0.$$

We find that

$$M = (q-1)^3-(q-1)(q-2)(q-3) = (q-1)(3q-5),$$

so that

$$\sum_{a,b} K^4(a,b) = q^2(q-1)(3q-5).$$

Finally

(7.8) $$\sum_{a\neq 0} K^4(a,1) = 2q^3-2q^2-3q-1,$$

so that

(7.9) $$K(a,1) = O(q^{3/4}) \quad (a \neq 0).$$

References

[1] L. Carlitz, *Weighted quadratic partitions over a finite field*, Canad. Journ. Math. 5 (1953), pp. 317-323.

[2] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, New York 1958.

Reçu par la Rédaction le 13. 5. 1968