Relationen zwischen verallgemeinerten Gaußschen Summen.

Von *Hermann Ludwig Schmid* in Göttingen.

---

k sei ein Galoisfeld von $q = p^f$ Elementen. $\chi(x)$, $\psi(x)$ seien Charaktere der Ordnungen m, n der Multiplikativgruppe von k.

$$e(x) = \mathsf{Z}^{\mathfrak{S}(x)} \qquad (\mathsf{Z} = e^{\frac{2\pi i}{p}},\ \mathfrak{S} \text{ absolute Spur von } k)$$

sei ein Charakter der Ordnung p der Additivgruppe von k. Dann sind die verallgemeinerten Gaußschen Summen durch

$$\tau(\chi) = -\sum_{x \neq 0}' \chi(x)\, e(x)$$

definiert.

$k^{(r)}$ sei das höhere Galoisfeld von q^r Elementen. Durch

$$\chi_r(y) = \chi(N_r(y)) \qquad (y \text{ in } k^{(r)},\ N_r \text{ die Relativnorm für } k^{(r)}/k)$$

wird ein Charakter χ_r von $k^{(r)}$ definiert. Dann sei $\tau^r(\chi_r)$ die mit dem Charakter χ_r in $k^{(r)}$ gebildete verallgemeinerte Gaußsche Summe.

Davenport und Hasse haben folgende interessante formale Relationen zwischen verallgemeinerten Gaußschen Summen aufgestellt [1]):

$$(1) \qquad \tau^r(\chi_r) = \tau(\chi)^r,$$

$$(2) \qquad \psi(m^m) \prod_{\mu=0}^{m-1} \tau(\chi^\mu \psi) = \tau(\psi^m) \prod_{\mu=1}^{m-1} \tau(\chi^\mu).$$

In der genannten Arbeit werden dafür zwei Beweise gegeben, die trotz des elementaren Charakters dieser Relationen schwierige Hilfsmittel benutzen (Klassenkörpertheorie bzw. Prinzip der arithmetischen Charakterisierung).

Ich gebe hier einen elementaren Beweis der Relation (1) und spreche eine Vermutung aus, deren Bestätigung auch einen elementaren Beweis der Relation (2) liefern würde.

1. Wir beweisen (1) durch Induktion nach r. Sei (1) schon für r als richtig erkannt. Dann ist

$$\begin{aligned}\tau(\chi)^{r+1} &= \tau(\chi)^r \tau(\chi) = \tau^r(\chi_r)\tau(\chi)\\ &= \sum_{\substack{x \text{ in } k\\ y \text{ in } k^{(r)}}}' \chi(xN_r(y))\, e(x + S_r(y)) \qquad (S_r \text{ die Relativspur für } k^{(r)}/k)\\ &= \sum_{u \text{ in } k}' \chi(u) \sum_{v \bmod p} \mathsf{Z}^v M(u, v),\end{aligned}$$

---

[1]) H. Davenport und H. Hasse, Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, Journ. f. Math. 172 (1934).

wo $M(u, \nu)$ die Anzahl der Lösungen (x, y) von

$$(3) \qquad \mathfrak{S}(x + S_r(y)) = \nu \quad \text{mit} \quad x N_r(y) = u \qquad \begin{pmatrix} x \text{ in } k, & x \neq 0 \\ y \text{ in } k^{(r)}, & y \neq 0 \end{pmatrix}$$

bedeutet.

Andererseits ist

$$\begin{aligned} \tau^{r+1}(\chi_{r+1}) &= -\sum_{z \text{ in } k^{(r)}}{}' \chi(N_{r+1}(z))\, e(S_{r+1}(z)) \\ &= -\sum_{u \text{ in } k}{}' \chi(u) \sum_{\nu \bmod p} \mathrm{Z}^{\nu} N(u, \nu), \end{aligned}$$

wo $N(u, \nu)$ die Anzahl der Lösungen z von

$$(4) \qquad \mathfrak{S}(S_{r+1}(z)) = \nu \quad \text{mit} \quad N_{r+1}(z) = u \qquad (z \text{ in } k^{(r+1)},\ z \neq 0)$$

bedeutet.

Daraus folgt

$$\tau(\chi)^{r+1} - \tau^{r+1}(\chi_{r+1}) = \sum_{u \text{ in } k}{}' \chi(u) \sum_{\nu \bmod p} \mathrm{Z}^{\nu}(M(u, \nu) + N(u, \nu)).$$

(1) wird auch für $r + 1$ richtig sein, wenn die Unabhängigkeit der Summe $M(u, \nu) + N(u, \nu)$ von u oder ν gezeigt ist. Der folgende Beweis liefert zugleich ihre Unabhängigkeit von beiden u und ν. (3) und (4) schreiben wir so:

$$(3\text{a}) \qquad f_u(y) = \sum_{i=0}^{f-1} \left(y + y^q + \cdots + y^{q^{r-1}} + \frac{u}{y^{1+q+\cdots+q^{r-1}}} \right)^{p^i} = \nu$$

$$(y \text{ in } k^{(r)},\ y \neq 0),$$

$$(4\text{a}) \qquad f_u(z) = \sum_{i=0}^{f-1} \left(z + z^q + \cdots + z^{q^{r-1}} + \frac{u}{z^{1+q+\cdots+q^{r-1}}} \right)^{p^i} = \nu \quad \text{mit} \quad N_{r+1}(z) = u$$

$$(z \text{ in } k^{(r+1)},\ z \neq 0).$$

Das letztere folgt aus $u = N_{r+1}(z) = z^{1+q+\cdots+q^{r-1}+q^r}$, also

$$z^{q^r} = \frac{u}{z^{1+q+\cdots+q^{r-1}}}.$$

$M(u, \nu)$ ist die Anzahl der Lösungen y von (3a), $N(u, \nu)$ die Anzahl der Lösungen z von (4a). Die rationale Funktion $f_u(t)$ auf den linken Seiten von (3a) und (4a) wird durch Multiplikation mit dem Nenner $t^{p^{f-1}(1+q+\cdots+q^{r-1})}$ ein Polynom $F_u(t)$. Der Grad von $F_u(t)$ ist

$$g = \frac{q}{p}\left(q^{r-1} + (1 + q + \cdots + q^{r-1})\right).$$

Daraus folgt, daß für jedes Paar u, ν die Anzahl der Lösungen von $f_u(t) = \nu$ im Körper $k^{(r(r+1))}$, der $k^{(r)}$ und $k^{(r+1)}$ als Unterkörper enthält, höchstens gleich g ist.

In $f_u(t)$ setzen wir nun die $q^r - 1$ Elemente $y \neq 0$ aus $k^{(r)}$ und die $\frac{q^{r+1} - 1}{q - 1}$ Elemente z aus $k^{(r+1)}$ mit $N_{r+1}(z) = u$ ein. Daraus folgt

$$\sum_{\nu \bmod p} (M(u, \nu) + N(u, \nu)) = q^r - 1 + \frac{q^{r+1} - 1}{q - 1}.$$

Der Mittelwert für ein festes u beträgt also

$$m = \frac{q}{p}\left(q^{r-1} + (1 + q + \cdots + q^{r-1})\right) = g.$$

Für den Fall, daß die in M und N gezählten Lösungen für ein festes u untereinander verschieden sind, folgt daraus $M(u, \nu) + N(u, \nu) = g$. Da $k^{(r)}$ und $k^{(r+1)}$ den Durchschnitt k haben, werden in M und N dann und nur dann gleiche Lösungen gezählt, wenn $u = w^{r+1}$ mit w aus k ist. Diese Lösungen w sind beim obigen Einsetzungsprozeß doppelt gezählt worden. Dafür treten diese Lösungen in $f_u(t) = \nu$ aber gerade als zweifache Wurzeln auf. Denn es ist

$$\frac{d}{dt}\left(f_u(t) - \nu\right) = 1 - \frac{u}{t^{2+q+\cdots+q^{r-1}}},$$

also $\frac{d}{dt}\left(f_u(t) - \nu\right) = 0$ für $t = w$ und $u = w^{r+1}$. Also ist auch in diesem Falle $M(u, \nu) + N(u, \nu) = g$, womit der Induktionsbeweis erbracht ist.

2. Die beiden Seiten der Relation (2) schreiben wir so:

$$\begin{aligned}\psi(m^m)\prod_{\mu=0}^{m-1}\tau(\chi^\mu\psi) &= (-1)^m \sum_{x_0, x_1, \ldots, x_{m-1}}{}' e(x_0 + x_1 + \cdots + x_{m-1})\,\psi(m^m x_0 x_1 \cdots x_{m-1})\,\chi(x_1 x_2^2 \cdots x_{m-1}^{m-1}) \\ &= (-1)^m \sum_{u \text{ in } k}{}' \psi(u) \sum_{\nu \bmod p} \mathrm{Z}^\nu A(u, \nu),\end{aligned}$$

wo

$$A(u, \nu) = \sum_{\substack{m^m x_0 x_1 \cdots x_{m-1} = u \\ \mathfrak{S}(x_0 + x_1 + \cdots + x_{m-1}) = \nu}}{}' \chi(x_1 x_2^2 \cdots x_{m-1}^{m-1}) \qquad \left(\begin{matrix} x_i \text{ in } k, & x_i \neq 0 \\ i = 0, 1, \ldots, m-1 \end{matrix}\right).$$

$$\begin{aligned}\tau(\psi^m)\prod_{\mu=1}^{m-1}\tau(\chi^\mu) &= (-1)^m \sum_{y_0, y_1, \ldots, y_{m-1}}{}' e(y_0 + y_1 + \cdots + y_{m-1})\,\psi(y_0^m)\,\chi(y_1 y_2^2 \cdots y_{m-1}^{m-1}) \\ &= (-1)^m \sum_{u \text{ in } k}{}' \psi(u) \sum_{\nu \bmod p} \mathrm{Z}^\nu B(u, \nu),\end{aligned}$$

wo

$$B(u, \nu) = \sum_{\substack{y_0^m = u \\ \mathfrak{S}(y_0 + y_1 + \cdots + y_{m-1}) = \nu}}{}' \chi(y_1 y_2^2 \cdots y_{m-1}^{m-1}) \qquad \left(\begin{matrix} y_i \text{ in } k, & y_i \neq 0 \\ i = 0, 1, \ldots, m-1 \end{matrix}\right).$$

Es liegt nun die Vermutung nahe, daß

$$(5) \qquad A(u, \nu) = B(u, \nu).$$

Dies ist lediglich eine Behauptung über den Charakter χ. Aus (5) würde sofort die Richtigkeit von (2) folgen.

Für $\chi(u) \neq 1$ können wir (5) sofort bestätigen. Denn dann ist einerseits $B(u, \nu) = 0$, andererseits $\chi(u) A(u, \nu) = A(u, \nu)$, d. h. $A(u, \nu) = 0$.

(5) braucht also nur noch für u mit $\chi(u) = 1$ bewiesen zu werden. Für $m = 2$ ist die Gültigkeit von (5) leicht einzusehen.

Eingegangen 7. Februar 1936.