Séminaire Lotharingien de Combinatoire, B33f (1994)

GAUSSCHE SUMMEN ÜBER ENDLICHEN KÖRPERN UND GAMMA FUNKTION

VON

ANNA HELVERSEN-PASOTTO

ABSTRACT. — Gaussian Sums over finite fields are analogous to values of the gamma function as can be seen via the Eulerian integral for the Gamma function. This seems to have been known to Gauss already; this seems to have been for him one of the reasons to introduce these sums. Nevertheless it has been astonishing for several authors to discover identities for Gaussian sums which bear a strong formal analogy with classical identities for the gamma function; also a p-adic gamma function has been invented and many of the well known classical identities have been shown to admit p-adic analogs. The aim of these lectures is to give an introduction to the subject discussing some identities, giving some proofs and pointing out relations to the representation theory of the general linear group of a finite field (Hecke algebras). The analogy between binomial coefficients and Jacobi sums leading to hypergeometric functions over finite fields is mentioned.

Inhalt

1. Einleitung. — Eine Gaussche Summe $G(A)$ ist eine gewisse komplexe Zahl, die einem multiplikativen Charakter A eines endlichen Körpers zugeordnet wird; die genaue Definition wird im nächsten Abschnitt angegeben. Diese Zahlen $G(A)$ verhalten sich in mancher Beziehung ähnlich wie die Werte $\Gamma(a)$ der Gammafunktion; z.B. bestehen zwischen solchen Gausschen Summen Beziehungen, die eine starke Analogie zu klassischen Identitäten für die Gammafunktion aufweisen. Einige dieser Identitäten werden im vierten Abschnitt diskutiert. Das Eulersche Integral für die Gammafunktion gibt einen Hinweis für das Verständnis dieser Analogien (siehe Abschnitt 3). Eine Theorie hypergeometrischer Reihen für den

Fall endlicher Körper lässt sich auf einer Analogie zwischen Binomialkoeffizienten und Jacobisummen aufbauen (siehe Abschnitt 5). Bei Wahl einer geeigneten Basis für eine irreduzible Darstellung der allgemeinen linearen Gruppe eines endlichen Körpers treten in den matriziellen Koeffizienten Gaussche Summen auf; die Relationen zwischen Gruppenelementen führen zu Identitäten zwischen Gausschen Summen; manch ein Analogon einer klassischen Identität lässt sich so "erklären", und umgekehrt kann man versuchen, durch diese Betrachtungsweise neue Identitäten zu gewinnen. Dies ist der Inhalt von Abschnitt 6 und 7.

Nur wenige Beweise werden angegeben; meist wird auf die Bibliographie verwiesen, wie auch für historische Hinweise. Dies ermöglicht, diese Vorträge auf nicht allzuvielen Seiten unterzubringen.

Die Verfasserin dankt den Organisatoren für diese angenehme Gelegenheit, zum Teil auch über ihre eigenen Forschungsresultate vorzutragen.

2. Gaussche Summen über endlichen Körpern. — Im Blick auf eine eventuelle Behandlung dieses Themas durch formales Rechnen (mit Maple, Reduce oder Mathematika...) möchte ich ein paar einfache Beweise ausführlich angeben. In allem folgendem wird ein einfaches Lemma immer wieder angewendet.

Lemma 1. — *Sei G eine endliche Gruppe, sei* $\mathrm{ord}(G)$ *die Anzahl der Elemente von G; sei $A : G \to \mathbb{C}^\times$ ein Gruppenmorphismus von G in die multiplikative Gruppe $\mathbb{C}^\times$ des Körpers $\mathbb{C}$ der komplexen Zahlen; dann gilt*

$$\sum_{g\in G} A(g) = \delta(A)\,\mathrm{ord}(G);$$

dabei ist das Kroneckersymbol $\delta(A)$ gleich 1, falls A konstant vom Wert ist, anderenfalls gleich Null.

Wir möchten einen einfachen und wohlbekannten Beweis angeben : Wenn alle Werte von A gleich Eins sind, so ist natürlich die Summe aller $A(g)$ über g aus G gleich der Anzahl $\mathrm{ord}(G)$ der Elemente von G. Anderenfalls gibt es ein x in G, so dass $A(x) \neq 1$; man hat

$$\sum_{g\in G} A(g) = \sum_{g\in G} A(xg) = A(x) \sum_{g\in G} A(g),$$

und es folgt

$$(1 - A(x)) \sum_{g\in G} A(g) = 0;$$

weil $1 - A(x) \neq 0$, folgt weiter $\sum_{g\in G} A(g) = 0$, was zu beweisen war.

Sei nun p eine Primzahl, dann ist $F_p = \mathbb{Z}/p\mathbb{Z}$ ein endlicher Körper; wie üblich, bezeichnet $\mathbb{Z}$ den Ring der ganzen Zahlen. Sei F_p^+ die additive Gruppe von F_p; durch

$$\begin{aligned} F_p^+ &\to \mathbb{C}^* \\ k \bmod p &\mapsto \exp(2\pi ik/p) \end{aligned}$$

wird ein Gruppenmorphismus definiert.

Sei nun $n \in \mathbb{Z}$, $n \geq 1$, $q = p^n$; man weiss, dass es bis auf Isomorphie genau einen endlichen Körper F_q mit q Elementen gibt, und man kennt die Spurabbildung

$$\begin{aligned} \mathrm{Spur} : F_q &\to F_p \\ x &\mapsto x + x^p + \cdots + x^{p^{n-1}}. \end{aligned}$$

Durch

$$\begin{aligned} E : F_q^+ &\to \mathbb{C}^\times \\ x &\mapsto \exp(2\pi \,\mathrm{Spur}(x)/p) \end{aligned}$$

wird ein Gruppenmorphismus von der additiven Gruppe F_q^+ in die multiplikative $\mathbb{C}^\times$ definiert; dieser ist nicht konstant vom Wert Eins, man sagt nichttrivial. Man nennt E den kanonischen nichttrivialen additiven Charakter von F_q. Die Werte von E sind p-te Einheitswurzeln.

Man betrachtet die multiplikative Gruppe $F_q^\times$ von F_q und Gruppenmorphismen $A : F_q^\times \to \mathbb{C}^\times$ genannt multiplikative Charaktere von F_q. Man definiert die *Gaussche Summe* $G(A)$ als

$$G(A) = \sum_{t \in F_q^\times} E(t)A(t).$$

Da $F_q^\times$ eine Gruppe von $q-1$ Elementen ist, ist jedes $A(t)$ eine $(q-1)$-te Einheitswurzel, $E(t)A(t)$ ist eine $p(q-1)$-te Einheitswurzel, und $G(A)$ ist ein Element des algebraischen Zahlkörpers $\mathbb{Q}(\exp(2(\pi i/(p(q-1)))$, der aus dem Körper $\mathbb{Q}$ der rationalen Zahlen durch Adjunktion der $p(q-1)$-ten Einheitswurzeln entsteht. Wir wollen ein paar einfache Eigenschaften von Gausschen Summen beweisen :

(1) Der absolute Betrag der Gausschen Summe $G(A)$ ist gleich der Quadratwurzel von q, falls A nicht konstant vom Wert Eins ist.

(2) Ist hingegen A konstant vom Wert Eins, so ist $G(A) = -1$.

(3) Für zwei multiplikative Charaktere A_1 und A_2, deren Produkt nicht konstant vom Wert 1 ist, hat man

$$G(A_1)G(A_2) = B(A_1, A_2)G(A_1A_2);$$

hierbei bezeichnet $B(A_1, A_2)$ die Jacobisumme von A_1 und A_2 ; diese ist folgendermassen definiert :

$$B(A_1, A_2) = \sum_{\substack{x+y=1 \\ x,y \in F_q^\times}} A_1(x) A_2(y).$$

Beweis von (1) :

$$\begin{aligned}\overline{G(A)}G(A) &= \sum_{s\neq 0} \overline{E(s)}\,\overline{A(s)} \sum_{t \neq 0} E(t)A(t) = \sum_{s,t\neq 0} E(t-s)A(s^{-1}t) \\ &= \sum_{u,s\neq 0} E(s(u-1))A(u) = \sum_{u\neq 0} A(u) \sum_{s \neq 0} E(s(u-1)).\end{aligned}$$

Nun wendet man Lemma 1 auf den folgenden Gruppenmorphismus an :

$$\begin{aligned} F_q^+ &\longrightarrow \mathbb{C}^\times \\ s &\longmapsto E(s(u-1)) \end{aligned}$$

und erhält so

$$\sum_{s\in F_q^+} E(s(u-1)) = \begin{cases} q, & \text{für } u = 1\,; \\ 0, & \text{für } u \neq 1\,; \end{cases}$$

und weiter

$$\sum_{s\neq 0} E(s(u-1)) = \begin{cases} q-1, & \text{für } u = 1\,; \\ -1, & \text{für } u \neq 1. \end{cases}$$

Es folgt $\overline{G(A)}G(A) = (q-1) - \sum_{u\neq 0,1} A(u)$; man wendet nochmal Lemma 1 an, diesmal für den Morphismus $A : F^\times \to \mathbb{C}^\times$ und erhält

$$\sum_{u\neq 0} A(u) = \begin{cases} q-1, & \text{für } A \text{ konstant gleich } 1\,; \\ 0, & \text{anderenfalls}\,; \end{cases}$$

das heisst

$$\sum_{u\neq 0,1} A(u) = \begin{cases} q-2, & \text{für } A \text{ konstant gleich } 1\,; \\ -1, & \text{anderenfalls.} \end{cases}$$

Es folgt nun

$$\overline{G(A)}G(A) = \begin{cases} q, & \text{für } A \text{ nicht konstant gleich } 1\,; \\ 1, & \text{anderenfalls}\,; \end{cases}$$

und damit ist (1) bewiesen.

Beweis von (2) : Nach Lemma 1 hat man $\sum_{t\in F_q^+} E(t) = 0$; es folgt $\sum_{t\neq 0} E(t) = -1$; für A konstant gleich Eins ist $G(A) = \sum_{t\neq 0} E(t)$, also $G(A) = -1$.

Beweis von (3) :

$$\begin{aligned} G(A_1)G(A_2) &= \sum_{t_1,t_2\neq 0} E(t_1+t_2)A_1(t_1)A_2(t_2) \\ &= \sum_{u,t_2\neq 0} E((u+1)t_2)(A_1A_2)(t_2)A_1(u) \\ &= \sum_{u\neq 0,-1} A_1(u)\sum_{t\neq 0} E((u+1)t)(A_1A_2)(t) + A(-1)\sum_{t\neq 0}(A_1A_2)(t). \end{aligned}$$

Da A_1A_2 nach Voraussetzung nicht konstant gleich Eins ist, findet man mit Lemma 1, dass der letzte Summand gleich Null ist. Durch Umparametrieren $(u+1)t = s$ erhält man :

$$\begin{aligned} G(A_1)G(A_2) &= \sum_{u\neq 0,-1} A_1(u)\sum_{s\neq 0} E(s)(A_1A_2)((u+1)^{-1}s) \\ &= \sum_{u\neq 0,-1} A_1(u)(A_1A_2)^{-1}(u+1)\sum_{s\neq 0} E(s)(A_1A_2)(s) \\ &= G(A_1A_2)\sum_{u\neq 0,-1} A_1\Big(\frac{u}{u+1}\Big)A_2\Big(\frac{1}{u+1}\Big) \\ &= G(A_1A_2)\sum_{\substack{x,y\neq 0\\ x+y=1}} A_1(x)A_2(y) \\ &= G(A_1A_2)B(A_1,A_2), \end{aligned}$$

was zu beweisen war.

3. Analogie zur Gammafunktion. — Die Eulersche Integralformel

$$\Gamma(a) = \int_0^\infty e^{-t}t^{a-1}dt, \quad a > 0,$$

zeigt eine Analogie von Gammafunktion und Gausschen Summen

$$G(A) = \sum_{t\in F_q^\times} E(t)A(t)$$

auf : offenbar verhält sich $t \mapsto e^{-t}$ additiv ($e^{-(s+t)} = e^{-s}e^{-t}$) und $t \mapsto t^{(a-1)}$ multiplikativ ($(st)^{a-1} = s^{a-1}t^{a-1}$); die Integration entspricht der Summation.

Die klassische Betafunktion

$$B(a_1, a_2) = \int_0^1 t^{a_1-1}(1-t)^{a_2-1}dt$$

entspricht den Jacobisummen

$$B(A_1, A_2) = \sum_{t\neq 0,1} A_1(t)A_2(1t),$$

und die klassische Identität

$$\Gamma(a_1)\Gamma(a_2) = B(a_1, a_2)\Gamma(a_1 + a_2), \quad a_1, a_2 > 0,$$

für Gamma und Betafunktion entspricht der im vorangehenden Abschnitt bewiesenen Identität zwischen Gausschen Summen und Jacobisummen

$$G(A_1)G(A_2) = B(A_1, A_2)G(A_1A_2), \quad A_1A_2 \text{ nichttrivial.}$$

Es stellt sich ganz natürlich die Frage : Wie sieht es mit anderen klassischen Identitäten aus ? Lassen diese sich auf den "endlichen" Fall übertragen ? In der Tat

$$\sin(\pi a)\Gamma(a)\Gamma(1-a) = \pi$$

lässt sich in

$$A(-1)G(A)G(A^{-1}) = q, \quad A \text{ nichttrivial,}$$

wiedererkennen ; der Spezialfall $a = 1/2$

$$\Gamma(1/2)^2 = \pi$$

entspricht

$$Q(-1)G(Q)^2 = q,$$

wobei Q den quadratischen Charakter bezeichnet, $Q(x) = 1$, falls x ein Quadrat in F_q ist, anderenfalls $Q(x) = -1$; wählt man einen Teichmüllercharakter τ, d.h. einen Erzeugenden für die Gruppe der multiplikativen Charaktere von F_q, so hat man

$$Q = \tau^{(q-1)/2}$$

für ungerades q ; für gerades q ist Q der triviale Charakter (jedes Element von F_q ist ein Quadrat).

Die Gaussche Multiplikationsformel

$$\prod_{j=1}^{k-1} \frac{\Gamma(a + j/k)}{\Gamma(j/k)} = k^{-ak}\frac{\Gamma(ak+1)}{\Gamma(a+1)}$$

entspricht der Multiplikationsformel von Hasse und Davenport :

$$\prod_{j=1}^{k-1} \frac{G(a+j(k-1)/k)}{G(j(q-1)/k)} = \tau(k)^{-ak} \frac{G(ak)}{G(a)}, \quad k/q-1;$$

hierbei ist abkürzend geschrieben $G(m)$ für $G(\tau^m)$ unter Benutzung eines Teichmüllercharakters τ.

Die Duplikationsformel (Spezialfall $k=2$)

$$\frac{\Gamma(a+1/2)}{\Gamma(1/2)} = 4^{-a} \frac{\Gamma(2a+1)}{\Gamma(a+1)}$$

entspricht

$$\frac{G(AQ)}{G(Q)} = A^{-1}(4) \frac{G(A^2)}{G(A)}.$$

4. Weitere Identitäten. — Anfang des Jahrhunderts wurde von Barnes beim Studium der Lösungen der hypergeometrischen Differentialgleichung das folgende Lemma bewiesen (Barnes' First Lemma) :

$$\frac{1}{2\pi i} \int_{-i\infty}^{+i\infty} \Gamma(a_1+s)\Gamma(a_2-s)\Gamma(a_3+s)\Gamma(a_4-s)\, ds = \frac{\Gamma(a_1+a_2)\Gamma(a_2+a_3)\Gamma(a_3+a_4)\Gamma(a_4+a_1)}{\Gamma(a_1+a_2+a_3+a_4)}$$

unter gewissen Einschränkungen an die Wahl des Integrationsweges und an die vier komplexen Zahlen a_1, a_2, a_3 und a_4.

Beim Studium der Gelfand-Graevschen Darstellung der Gruppe $GL(2, F_q)$ stiess 1978 die Verfasserin auf das folgende Lemma für Gaussche Summen :

$$\frac{1}{q-1} \sum_{S \in X} G(A_1 S) G(A_2 S^{-1}) G(A_3 S) G(A_4 S^{-1}) = \frac{G(A_1 A_2) G(A_2 A_3) G(A_3 A_4) G(A_4 A_1)}{G(A_1 A_2 A_3 A_4)};$$

hier ist mit X die Menge (Gruppe) der multiplikativen Charaktere von F_q bezeichnet ; A_1, A_2, A_3, A_4 sind in X, und es wird vorausgesetzt, dass das Produkt $A_1 A_2 A_3 A_4$ nicht konstant gleich Eins ist (anderenfalls kann die Identität aber leicht korrigiert werden durch Hinzufügen eines Kroneckersymbols $\delta(A_1 A_2 A_3 A_4)$ multipliziert mit gewissen Konstanten und Charakterwerten).

Dieses Lemma entspricht den Darstellungen der Hauptreihe von $GL(2, F_q)$; die diskrete Reihe hingegen führt zu einer Identität, in der multiplikative Charaktere des Körpers F_{q^2} von q^2 Elementen vorkommen (quadratische Erweiterung von F_q); für alles genauere sei auf die Artikel [HP 78], [HP 86] und [HP 91] verwiesen. Für einen kurzen direkten Beweis dieses Lemmas, der im wesentlichen nur Lemma 1 benutzt, sei auf [HP 93] verwiesen. Für einen kompliziertern Beweis der aber gleichzeitig auch einen neuen Beweis des klassischen Barnes' First Lemma liefert über Umparametrisierungen in den Integralformeln sei auf [HP-PS 93] verwiesen.

Es sei dieser Abschnitt abgeschlossen mit einem kurzen Bericht über die berühmte Selbergsche Integralformel und ihr "endliches Analogon". Diese Formel ist eine Verallgemeinerung der Identität zwischen Gamma und Betafunktion und wurde 1944 von Selberg veröffentlicht :

$$\int_0^1 \dots \int_0^1 (t_1 \dots t_n)^{a-1}((1-t_1)\dots(1-t_n))^{b-1}\Delta_n^c \, dt_1 \dots dt_n \\ = n! \prod_{j+0}^{n-1} \frac{\Gamma(a+jc)\Gamma(b+jc)\Gamma(c+jc)}{\Gamma(c)\Gamma(a+b+c(n+j-1)},$$

wobei $\mathrm{Re}(a)$, $\mathrm{Re}(b)$, $\mathrm{Re}(c) > 0$ und $\Delta_n = \prod_{1 \leq i \leq j \leq n} (t_i - t_j)^2$.

Schon damals beschäftigte sich Selberg mit Analogien für Gaussche Summen und bewies gewisse Identitäten, ohne diese zu veröffentlichen [Ev 81]. Erst 1990 wurde die folgende allgemeine Formel für Gaussche Summen bewiesen

$$\sum_F \tau((-1)^{na}F(0)^a F(1)^b \Delta_F^c) Q(\Delta_F) \\ = \prod_{j=0}^{n-1} \frac{G'(a+jc)G'(b+jc)G'(c+jc)}{G'(c)G'(a+b+c(n+j-1)},$$

wobei summiert wird über alle unitären Polynome F über F_q vom Grad n und wobei Δ_F die Diskriminante von F bezeichnet; wie in den vorangehenden Abschnitten bezeichnet τ einen Teichmüllercharakter und Q den quadratischen Charakter von F_q; die ganzen Zahlen a, b und c unterliegen gewissen Einschränkungen; die Gausschen Summen $G'(m)$ sind im wesentlichen die Gausschen Summen des multiplikativen Charakters τ^{-m} für ganze Zahlen m; für alle Einzelheiten und Beweise sei auf [An 90] und [Ev 91] verwiesen.

Die Beschäftigung mit dem "endlichen Analogon" hat Anderson zu einem neuen kurzen Beweis der ursprünglichen Selbergschen Integralformel geführt [An 91] . Diese Art von Resultaten kann man wohl als "Rechtfertigung" des Interesses für den endlichen Fall auffassen, falls man solch eine braucht. Eine geometrische Interpretation der "Selberg Evans

Summe" (linke Seite der vorangehenden Formel) und ein kohomologischer Beweis der Formel wurde von Denef und Loeser gefunden [De-Lo 94].

5. Binomialkoeffizienten, Jacobisummen und hypergeometrische Funktionen über endlichen Körpern. — Für ganze Zahlen, grösser Null, ist $\Gamma(n) = (n-1)!$, und man kann die Gausschen Summen $G(A)$ in Analogie zu n ! sehen. Sei, wie im vorangehenden Abschnitt mit X die Gruppe der multiplikativen Charaktere von F_q bezeichnet. Wir wollen "Binomialkoeffizienten" $\binom{A}{S}$ definieren für A und S in X. Für n, k ganze Zahlen, $0 < k < n$, hat man $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ und man wäre versucht $\binom{A}{S}$ gleich $\frac{G(A)}{G(S)G(A/S)}$ zu setzen. Durch einen hübschen Trick beweist J. Greene den folgenden Binomialsatz : für A in X und x in F_q hat man

$$A(1+x) = \Delta(x) + \frac{1}{q-1}\sum_S B(A, S^{-1})S(-x)$$

offenbar analog zu

$$(1+x)^a = \sum_{s=0}^{a} \binom{a}{s} x^s \quad \text{für natürliche Zahlen } a.$$

Man hat $S^{-1}(x) = \overline{S(x)}$, da $S(x)$ eine $(q-1)$−te Einheitswurzel ist ; statt S^{-1} kann man daher auch $\overline{S}$ schreiben und definieren :

$$\binom{A}{S} = \frac{S(-1)}{q-1} B(A, \overline{S})$$

Wie im zweiten Abschnitt bezeichnet B die Jacobisumme (analog zur Betafunktion). Der "Binomialsatz" nimmt dann die gewünschte Form an :

$$A(1+x) = \Delta(x) + \sum_S \binom{A}{S} S(x);$$

es sei nicht vergessen zu bemerken, dass $\Delta(x) = 0$ für $x \neq 0$ und $\Delta(x) = 1$ für $x = 0$, $S(0) = 0$ für alle S in X (per Definition). Benutzt man weiter das Kroneckersymbol $\delta(S) = 1$ für S konstant vom Wert 1 und $\delta(S) = 0$ anderenfalls, wobei S in X sei, so kann man sehen, dass

$$\binom{A}{S} = \frac{G(A)}{G(S)G(A, \overline{S})} + \frac{q-1}{q}\delta(S) + \frac{q-1}{q}\delta(A, \overline{S}).$$

Es verhalten sich diese Binomialkoeffizienten zu den Gausschen Summen "fast" so wie die normalen Binomialkoeffizienten zur "Faktoriellen." Die Reihenentwicklung der Exponentialfunktion

$$e^x = \sum_{s=0}^{\infty} \frac{1}{\Gamma(s+1)} x^s$$

entspricht der “Entwicklung” des kanonischen nichttrivialen additiven Charakters E durch die Formel

$$E(-x) = 1 + \frac{q}{q-1} \sum_S \frac{1}{G(S)} S(x).$$

Analog zur klassischen Situation führt J. Greene die “endliche hypergeometrische Reihe” ${}_2F_1$ ein als

$${}_2F_1\left({}^{A\,B}_{\ \,C}|x\right) = \frac{q}{q-1} \sum_S \binom{AS}{S} \binom{BS}{CS} S(X)$$

und erhält die “Integralformel”

$${}_2F_1\left({}^{A\,B}_{\ \,C}|x\right) = 1(x) \frac{(BC)(-1)}{q} \sum_y B(y)(\overline{B}C)(1-y)\overline{A}(1-xy);$$

hier bezeichnet 1 den multiplikativen Charakter von F_q, welcher für alle x mit $x \neq 0$ gleich 1 ist, während $1(0) = 0$. Mit Hilfe der “Gausschen Auswertung”

$${}_2F_1\left({}^{A\,B}_{\ \,C}|1\right) = A(-1) \binom{B}{\overline{A}C}$$

gewinnt J. Greene das in Abschnitt 4 diskutierte “endliche Barnes' First Lemma”. Mit Hilfe weiterer Auswertungen erhält er “endliche” Saalschütz, Dixon, Watson, Whipple Identitäten. Für alle Einzelheiten sei auf [Gr 87] verwiesen.

6. Darstellungen von $GL(n, F_q)$ und Identitäten von Gaussschen Summen. — Nach einem Satz von S.I. Gelfand ist die Einschränkung jeder Darstellung der “diskreten Reihe” von $GL(n, F_q)$ auf eine gewisse Untergruppe H irreduzibel und isomorph zu einer leicht konstruierbaren Darstellung t; genauer : H ist im wesentlichen die affine Gruppe $\mathrm{Aff}(n-1, F_q)$ und t ist die induzierte Darstellung $\mathrm{Ind}_U^H(t_E)$ mit

$$t_E \begin{pmatrix} 1 & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & 1 & a_{23} & \dots & a_{2n} \\ & & & & \\ & & & & a_{n-1,n} \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix} = E(a_{12} + \cdots + a_{n-1,n});$$

U wird von der Menge der hier angegebenen Matrizen gebildet (unipotente Untergruppe), t_E ist eindimensional, E ist der kanonische nichttriviale additive Charakter von F_q.

Die Darstellungen der diskreten Reihe von $GL(n, F_q)$ entsprechen im wesentlichen den multiplikativen Charakteren des endlichen Körpers F mit q^n Elementen. Die Charaktere dieser Darstellungen sind bekannt; sei T_Λ solch eine Darstellung; sei χ_Λ ihr Charakter, sei Λ der entsprechende multiplikative Charakter von F. Dann kann man "im Prinzip" alle Operatoren $T_\Lambda(g)$ für $g \in G$, $G = GL(n, F_q)$, mit Hilfe von t und χ_Λ berechnen (siehe [HP 82]).

Für $a \in F_q^\times$ sei $c(a)$ die Skalarmatrix mit a auf der Diagonalen und Null sonst überall; die Elemente der Gruppe H können als Matrizen geschrieben werden, deren unterste Linie gleich $(00\dots01)$ ist; weiter sei w das folgende Element der "Weylgruppe"

$$\begin{pmatrix} 1 & 0 & \dots & \dots & 0 & 0 \\ 0 & 1 & & & 0 & 0 \\ . & . & & & & \\ . & . & . & & . & . \\ & & & 1 & 0 & 0 \\ 0 & 0 & \dots & & 0 & 1 \\ 0 & 0 & \dots & \dots & 1 & 0 \end{pmatrix}$$

die Gruppe $GL(n, F_q)$ wird erzeugt durch H, die Skalarmatrizen und w mit gewissen Relationen. Wählt man für den Raum der Darstellung t eine geeignete Basis, so treten in den matriziellen Koeffizienten der Operatoren $T_\Lambda(g)$ Gaussche Summen auf. Gewisse Relationen für $T_\Lambda(w)$ führen zu interessanten Identitäten, z.B. zu einem Analogon der klassischen Dixon Identität. Für alle Einzelheiten sei auf [HP 82] und [HP 94] verwiesen.

7. Heckealgebren und Identitäten. — Sei G eine endliche Gruppe und H eine Untergruppe von G; sei $\mathbb{C}$ der Körper der komplexen Zahlen und $\mathbb{C}H$ die Gruppenalgebra von H über $\mathbb{C}$, sei e ein idempotentes Element in $\mathbb{C}H$, sei $\psi : H \to \mathbb{C}$ der Charakter der Darstellung von H auf dem Linksmodul $\mathbb{C}Ge$; dann ist $\mathbb{C}Ge$ isomorph zur induzierten Darstellung von H nach G der Darstellung (Linksmodul) $\mathbb{C}He$; der Charakter von $\mathbb{C}Ge$ ist ψ^G (der von H nach G induzierte Charakter von ψ). Ist ξ ein irreduzibler Charakter von G, so hat man

$$\langle \zeta, \psi^G \rangle = \psi(e),$$

d.h. das Skalarprodukt von ζ und ψ^G ist gleich dem Wert von ψ auf dem Element e aus $\mathbb{C}H$.

Man schreibt :

$$\mathcal{H}(G, H, \psi) := e\mathbb{C}Ge$$

und nennt diese Algebra die Heckealgebra von G, H, und ψ; diese ist antiisomorph zur Endomorphismenalgebra der induzierten Darstellung $\mathrm{Ind}_H^G(\lambda)$, wenn λ die Darstellung von H in $\mathbb{C}Ge$ bezeichnet.

Anhand der Doppelklassen von H in G lässt sich die Heckealgebra explizit beschreiben. Sei $x_1, \ldots, r_r$ ein Repräsentantensystem der Doppelklassen HxH von H in G; d.h. $G = Hx_1H \cup \cdots \cup Hx_rH$ (disjunkte Vereinigung), $Hx_iH \cap Hx_jH = \emptyset$ für $i \neq j$. Man setzt

$$e = (\operatorname{ord} H)^{-1} \sum_{h \in H} \psi(h^{-1})h;$$

e ist Idempotentes in $\mathbb{C}H$ und ψ ist der Charakter der Darstellung von H in $\mathbb{C}He$. Sei

$$J = \{j \in \{1, \ldots, r\} \mid |\psi(x_j^{-1}hx_j) = \psi(h) \,\text{für jedes}\, h \in H \cap x_jHx_j^{-1}\};$$

für $j \in J$ sei $\operatorname{ind}(x_j)$ der Index von $H \cap x_jHx_j^{-1}$ in H; sei

$$a_j = \operatorname{ind}(x_j)ex_je;$$

dann bilden die Elemente a_j (mit $j \in J$) eine Basis der Heckealgebra $\mathcal{H}(G, H, \psi)$;

Multipliziert man a_i mit a_j, so erhält man gewisse Koeffizienten μ_{ijk} durch

$$a_ia_j = \sum_{k \in J} \mu_{ijk}a_k;$$

diese Koeffizienten lassen sich berechnen als :

$$\mu_{ijk} = \operatorname{ord} H \sum_{y \in Hx_iH \cap x_kHx_j^{-1}H} a_i(y)a_j(y^{-1}x_k);$$

dabei sind die $a_m(u)$ definiert durch $a_m = \sum_{u \in G} a_m(u)u$; man nennt $(a_j)_{j \in J}$ "eine Standardbasis" der Heckealgebra $\mathcal{H}(G, H, \psi)$, und man nennt die komplexen Zahlen μ_{ijk} Strukturkonstanten der Heckealgebra. Wir wollen die Situation durch das folgende Beispiel illustrieren : $G = GL(2, F)$, $F = F_q$, $H = CU$ mit U unipotente Untergruppe, gebildet von allen Matrizen der Form

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \quad \text{mit}\, b \in F,$$

C Zentrum, gebildet von allen Skalarmatrizen $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ mit $a \in F^\times$, $\psi : H \to \mathbb{C}$ gegeben durch $\psi\left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\right) = A(a)E(b)$ für $a, b \in F$,

$a \neq 0$; dabei ist A ein multiplikativer Charakter von F_q und E ist der kanonische nichttriviale additive Charakter.

Wir benutzen die "Bruhatsche" Zerlegung der Gruppe zur Beschreibung der Doppelklassen; sei D die von allen Matrizen der Form $\begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}$ mit $d \in F$, $d \neq 0$, gebildete Untergruppe; sei $z = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; dann ist

$$G = CUD \cup CUDzU;$$

sei $x_c = \begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix}$ und $y_c = \begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix} z = \begin{pmatrix} 0 & c \\ 1 & 0 \end{pmatrix}$ für $c \in F$, $c \neq 0$; all diese Elemente zusammen bilden ein Repräsentantensystem der Doppelklassen von H in G. Das idempotente Element e von $\mathbb{C}H$, welches ψ entspricht, wird gegeben durch

$$e = \frac{1}{q(q-1)} \sum_{\substack{a,b \in F \\ a \neq 0}} A(a^{-1})E(-b) \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix};$$

man sieht leicht, dass $e = \operatorname{ind}(x_1)ex_1e$; wir wollen e mit a_0 bezeichnen und haben damit das "erste" Element unserer "Standardbasis" $(a_j)_{j \in J}$; dieses Element a_0 ist das Einselement unserer Heckealgebra $\mathcal{H}(G, H, \psi)$. Die Repräsentanten x_c mit $c \neq 1$ liefern keine Elemente für die Standardbasis, da sie die auf der vorangehenden Seite oben angegebene Bedingung an x_j nicht erfüllen. Hingegen alle y_c erfüllen diese Bedingung; wir setzen

$$a_c = \operatorname{ind}(y_c)ey_ce \quad \text{für } c \in F, c \neq 0$$

und erhalten so mit $(a_b)_{b \in F}$ eine Standardbasis (dabei ist $a_0 = e$ mit eingeschlossen). Man kann die Strukturkonstanten explizit berechnen und erhält

$$\mu_{ijk} = \sum_{c^2 = k/(ij)} A(c^{-1})E(c(i+j) - c^{-1})$$

für $i, j, k \neq 0$. Wir geben hier die Werte für $i, j, k = 0$ nicht an, sondern verweisen auf [HP 91], wie auch für alle Beweise, Literaturhinweise, usw.

Wir bezeichnen wie in den vorangehenden Abschnitten mit X die Gruppe der multiplikativen Charaktere von F und führen eine "neue" Basis der Heckealgebra ein, deren Elemente durch

$$a_S = \frac{1}{q-1} \sum_{c \neq 0} S(c)a_c$$

gegeben sind, für $S \in X$; jedes a_S ist also eine Linearkombination der a_c; das Basiselement a_0 wird beibehalten; sei $X' = \{0\} \cup X$, unsere neue Basis ist $(a_S)_{S \in X'}$, und wir können die Strukturkonstanten $\mu_{B,C,S}$ bezüglich der neuen Basis berechnen; diese drücken sich folgendermassen durch Gaussche Summen aus :

$$\begin{aligned} a_B a_C = & \frac{1}{q(q-1)} \delta(ABC) a_0 \\ & + \frac{(ABC)(-1)}{q(q-1)^2} G(ABC) \sum_{S \in X} S(-1) G(BS^{-1}) G(CS^{-1}) a_S; \end{aligned}$$

$$\mu_{B,C,S} = \begin{cases} \dfrac{\delta(ABC)}{q(q-1)}, & \text{für } B, C \in X \text{ und } S = 0; \\ \dfrac{(ABC)(-1)}{q(q-1)^2} G(ABC) G(BS^{-1}) G(CS^{-1}), & \text{für} B, C, S \in X; \end{cases}$$

es sei darauf hingewiesen, dass in diesen Formeln A den ein für alle mal festgelegten "zentralen" Charakter bezeichnet, der in die Definition von ψ eingeht (am Anfang des Beispiels).

Sei nun $\chi : G \to \mathbb{C}$ der Charakter einer irreduziblen Darstellung der Gruppe G, so dass $\chi(e) = 1$; dann ist $\chi : \mathcal{H} \to \mathbb{C}$ ein Algebramorphismus; es sei darauf hingewiesen, dass $\chi : G \to \mathbb{C}$ sich linear als $\chi : \mathbb{C}G \to \mathbb{C}$ fortsetzt und dann auf die Untermenge $\mathcal{H} = e\mathbb{C}Ge$ einschränkt.

Man hat daher für solch ein χ insbesondere $\chi(a_B a_C) = \chi(a_B)\chi(a_C)$, und aus $a_B a_C = \sum_{s \in X'} \mu_{B,C,S} a_S$ folgt weiter

$$\chi(a_B)\chi(a_C) = \sum_{S \in X'} \mu_{B,C,S} \chi(a_S).$$

Nun kann man die bekannte Charaktertafel der Gruppe $GL(2, F_q)$ verwenden, um ganz explizit in die letzte Formel die Werte $\chi(a_B)$, $\chi(a_C)$ und $\chi(a_S)$ einzusetzen.

Dies führt für die sogenannte "Hauptreihe" von Darstellungen genau auf die Barnesidentität (Seite 7); für die diskrete Reihe führt es auf neue interessante Identitäten. Für eine genaue Formulierung dieser Identitäten, wie auch für alle Beweise sei auf [HP 91] und die dort angegebene Literatur verwiesen.

LITERATURHINWEISE

[An 90] ANDERSON (Greg W.). — The evaluation of Selberg Sums, *C.R. Acad. Sc. Paris*, vol. **311**, 1990, p. 469–472.

[An 91] ANDERSON (Greg W.). — A short Proof of Selberg's Generalized Beta Formula, *Forum Mathematikum*, vol. **3**, 1991, p. 415–417.

[De-Lo 94] DENEF (J.) et LOESER (F.). — Détermination géométrique des sommes de Selberg-Evans, *Bull. Soc. Math. France*, vol. **122**, 1994, p. 533–551.

[Ev 81] EVANS (Ronald J.). — Identities for Products of Gauss Sums over Finite Fields, *Ens. Math.*, vol. **27**, 1981, p. 197–209.

[Ev 91] EVANS (Ronald J.). — The Evaluation of Selberg Character Sums, *Ens. Math.*, vol. **37**, 1991, p. 235–248.

[Gr 87] GREENE (John). — Hypergeometric Functions over Finite Fields, *Trans. Amer. Math. Soc.*, vol. **301**, 1987, p. 77–101.

[HP 78] HELVERSEN-PASOTTO (Anna). — L'identité de Barnes pour les corps finis, *C. R. Acad. Paris*, vol. **286**, 1978, p. 297–300.

[HP 82] HELVERSEN-PASOTTO (Anna). — Darstellungen von $GL(3, F_q)$ und Gaussche Summen, *Math. Ann.*, vol. **260**, 1982, p. 1–21.

[HP 86] HELVERSEN-PASOTTO (Anna). — Representation de Gelfand-Graev et identités de Barnes, le cas de $GL(2, F_q)$, *Ens. Math.*, vol. **32**, 1986, p. 57–77.

[HP 91] HELVERSEN-PASOTTO (Anna). — On the Structure Constants of certain Hecke algebras, *Rend. Circ. Mat. Palermo*, Serie II, numero 26, 1991.

[HP 93] HELVERSEN-PASOTTO (Anna). — Gamma-Function and Gaussian-Sum-Function, *Rend. Circ. Mat. Palermo*, Serie II, numero 30, 1993.

[HP-PS 93] HELVERSEN-PASOTTO (Anna) et SOLE (Patrick). — Barnes' First Lemma and its Finite Analogue, *Canad. Math. Bull.*, vol. **36**, 1993, p. 273–282.

[HP 94] HELVERSEN-PASOTTO (Anna). — Character Sum Identities in Analogy with Special Functions Identities, Université de Nice Sophia Antipolis, Imprimerie Maths, Prépublication no. 342, 1993 (zur Veröffentlichung umgearbeitet 1994).

Anna HELVERSEN-PASOTTO,
Laboratoire "Jean-Alexandre Dieudonné",
Mathématiques,
Université de Nice Sophia Antipolis,
Parc Valrose, B.P. 71,
F-06108 Nice Cedex 2.
email : `helpa@math.unice.fr`