Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 27 (1981)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: IDENTITIES FOR PRODUCTS OF GAUSS SUMS OVER FINITE FIELDS

Autor: Evans, Ronald J.

Kapitel: 2. Notation and the identities

DOI: https://doi.org/10.5169/seals-51748

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 19.08.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

and

(1b) $$\frac{1}{(2\pi)^{n/2}} \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} e^{-\frac{1}{2}(t_1^2 + \ldots + t_n^2)} \Delta_n^z \, dt_1 \ldots dt_n = n! \prod_{j=0}^{n-1} \frac{\Gamma(jz+z)}{\Gamma(z)}.$$

Identities (4), (4a) and (4b) were discovered and proved by A. Selberg in the early 1940's (unpublished). Also, essentially all of the material in §8 was known to Selberg. We are indebted to him for the ideas provided in [7].

Identity (5) was inspired by the case $n = 2$ of an integral formula of Andrews [1, (4.3)] somewhat similar to (1). It would be interesting to find a higher dimensional analogue.

2. Notation and the identities

Let p be prime and let $\zeta = \exp(2\pi i/p)$. Define the Gauss sum over $GF(p^r)$ by

$$G(\chi) = G_r(\chi) = -\sum_{x \in GF(p^r)} \chi(x)\, \zeta^{T(x)}$$

(note the minus sign), where T is the trace map from $GF(p^r)$ to $GF(p)$, and χ is any character on the multiplicative group of $GF(p^r)$ (with $\chi(0) = 0$). Fix a prime power $q = p^f$, $f \geqslant 1$.

It is proved in §4 that

(2) $$1 = \frac{\chi^l(l)\, G_f(\chi)}{G_f(\chi^l)} \prod_{j=1}^{e} \prod_{k=1}^{r} \prod_{c=1}^{w^{r-k}} \frac{G_{fn}\left(\chi^{\frac{q^n-1}{q-1}} \psi^{w^{k-1}(cw+i_j)}\right)}{G_{fn}\left(\psi^{w^{k-1}(cw+i_j)}\right)}$$

where $l = w^r$ for a prime $w \neq p$; n is the order of $q \pmod{w}$; $e = (w-1)/n$; $i_1, \ldots, i_e$ are coset representatives for the cyclic subgroup $\langle q \rangle$ in the multiplicative group of $GF(w)$; χ is a character on $GF(q^n)$; and ψ is a character of order l on $GF(q^n)$.

It is proved in §5 that

(3) $$1 = \frac{G_f(\chi^\alpha)}{\chi^\alpha(l)\, G_{fl}(\chi^{\alpha\beta})} \prod_{j=1}^{l-1} G_f(\chi^{j(q-1)/l}),$$

where $l \mid (q-1)$; α is an integer prime to l; β is the integer $(1+q+\ldots+q^{l-1})/l$; and χ is a character on $GF(q^l)$ of order $q^l - 1$. One comparing (3) with the last identity in [2, p. 368] should note that the exponent l on the last line of that page should be deleted; in fact, $(\text{Teich } l)^l\, a\,(q-1)$ should be corrected to read $(\text{Teich } l)^{a(q-1)}$. We remark that the product over j in (3) equals $q^{(l-1)/2}\, U_0$, where U_0 equals 1 or $i^{(p-1)^2 f/4}\,(-1)^{f+(q-1)(l-2)/8}$ according as l is odd or even. This fact is easy to prove for odd l (since $G_f(\psi)\, G_f(\overline{\psi}) = \psi(-1)\, q$ for a nontrivial character ψ on $GF(q)$); for even l, this follows from the classical evaluation of quadratic Gauss sums over $GF(p)$ (extended to $GF(q)$ via (6) below).

It is proved in §6 that

$$\sum_{x,\, y\in GF(q)} \chi_1(xy)\, \chi_2\big((1-x)(1-y)\big)\, \chi_3^2(x-y) = R(\chi_1, \chi_2, \chi_3) + R(\chi_1, \chi_2, \chi_3\phi), \tag{4}$$

where $\chi_1, \chi_2, \chi_3, \phi$ are characters on $GF(q)$; ϕ has order 2 (so $p > 2$); $\chi_1\chi_2\chi_3^2$ and $(\chi_1\chi_2\chi_3)^2$ are nontrivial; and

$$R(\chi_1, \chi_2, \chi_3) = \frac{G(\chi_3^2)\, G(\chi_1)\, G(\chi_1\chi_3)\, G(\chi_2)\, G(\chi_2\chi_3)}{G(\chi_3)\, G(\chi_1\chi_2\chi_3)\, G(\chi_1\chi_2\chi_3^2)}.$$

(Cf. (1)). The special case of (4) where $\chi_1 = \chi_2 = \chi_3^2 = \phi$ has been applied in graph theory [4], [9].

Selberg has pointed out that if χ, ψ, and ϕ are characters on $GF(q)$, where ϕ has order 2, then

$$\sum_{x,\, y\in GF(q)} \psi(xy)\, \chi^2(x-y)\, \zeta^{T(x+y)} = \frac{G(\psi)\, G(\chi\psi)\, G(\chi^2)}{G(\chi)} + \frac{G(\psi)\, G(\chi\psi\phi)\, G(\chi^2)}{G(\chi\phi)} \tag{4a}$$

and

$$\frac{1}{G^2(\phi)} \sum_{x,\, y\in GF(q)} \chi^2(x-y)\, \zeta^{\frac{p+1}{2} T(x^2+y^2)} = \frac{G(\chi^2)}{G(\chi)} + \frac{G(\chi^2)}{G(\chi\phi)}. \tag{4b}$$

These are character sum analogues of (1a) and (1b), respectively, for $n = 2$. We omit the proofs, as they are similar to (and easier than) the proof of (4).

It is proved in §7 that

$$\sum_{\substack{x,\, y\in GF(q)\\ x,\, y\neq 0}} \chi_1\chi_3\left(\frac{1+x}{y}\right) \chi_2\chi_3\left(\frac{1+y}{x}\right) \chi_1\chi_2(y-x) = D(\chi_1, \chi_2, \chi_3) + D(\chi_1\phi, \chi_2\phi, \chi_3\phi), \tag{5}$$

where $\chi_1, \chi_2, \chi_3, \phi$ are characters on $GF(q)$; ϕ has order 2 (so $p > 2$); $\chi_1^2, \chi_2^2, \chi_3^2, \chi_1\chi_2, \chi_1\chi_3$, and $\chi_2\chi_3$ are nontrivial; and

$$D(\chi_1, \chi_2, \chi_3) = \frac{q^2 \chi_2(-1)\, G(\chi_1\chi_2\chi_3)}{G(\chi_1)\, G(\chi_2)\, G(\chi_3)}.$$