有限線型群のガウス和

上智大学数学科

篠田健一

1. Gaussian sums

ガウスは Disquisitiones Arithmeticae (1801) の中で次の和を考察した.

$$G_p = \sum_{k=0}^{p-1} e^{2\pi i k^2/p}$$

ここで p は奇素数, $i = \sqrt{-1}$ である. $G_p = \pm\sqrt{p}$ (resp.$\pm i\sqrt{p}$) ($p \equiv 1 (\mathrm{mod}\, 4)$) (resp.($p \equiv 3 (\mathrm{mod}\, 4)$)) であることも記してある (356 章). しかし, この符号 (どちらも+) を定めるにはガウスも 4 年間を要したという. G_p はガウス和とよばれる.

G. L. Dirichlet (1840) は算術級数の素数定理の証明のため次の和を導入した.

$$G_n(\chi) = \sum_k \chi(k) e^{2\pi i k/n}$$

ここで n は正整数で χ は n を法とする乗法的な指標, k は n と互いに素な代表系のみ動く. χ_L を 法 p の Legendre 指標,

$$\chi_L(k) = \begin{cases} 1 & k \text{ が法 } p \text{ で平方数} \\ -1 & k \text{ が法 } p \text{ で非平方数} \end{cases}$$

とすると $G_p = G_p(\chi_L)$ が成立する. よって $G_n(\chi)$ もガウス和とよばれる.

さらに $e^{2\pi i(k+l)/n} = e^{2\pi i k/n} e^{2\pi i l/n}$ なので, p 元よりなる有限体 $\mathbb{F}_p$ の乗法的な指標, および加法的な指標の組 (χ, ψ) に対し

$$G_p(\chi, \psi) = \sum_{k=1}^{p-1} \chi(k)\psi(k)$$

も $\mathbb{F}_p$ 上のガウス和とよばれる. ここでは, この $\mathbb{F}_p$ を有限線型群として得られる結果について報告する.

この方向での一般化はガウス和に関係する膨大な論文の累積の中ではごく一部である. ガウス和全般に渡ることについては, 例えば入門的な総合報告である Berndt, Evans, Williams の共著 [1] をご覧いただきたい.

2. A GENERALIZATION

まず自然な拡張は, 素体 $\mathbb{F}_p$ を任意の有限体にすることである. $\mathbb{F}_q$ を $\mathbb{F}_p$ の m 次拡大体とする. $N_{\mathbb{F}_q/\mathbb{F}_p}:\mathbb{F}_q \to \mathbb{F}_p,\ x \mapsto x^{1+p+\cdots+p^{m-1}}$ をノルム写像, $T_{\mathbb{F}_q/\mathbb{F}_p}:\mathbb{F}_q \to \mathbb{F}_p,\ x \mapsto x+x^p+\cdots+x^{p^{m-1}}$ をトレースとする. このとき $\mathbb{F}_p$ の乗法的な指標, および加法的な指標の組 (χ,ψ), $(\psi \neq 1)$, に対し $(\chi \circ N_{\mathbb{F}_q/\mathbb{F}_p}, \psi \circ T_{\mathbb{F}_q/\mathbb{F}_p})$ は $\mathbb{F}_q$ の乗法的な指標, および加法的な指標の組を与える. 一般に $\mathbb{F}_q$ の乗法的な指標, および加法的な指標の組 (χ',ψ') に対し

$$G_q(\chi',\psi') = \sum_{x\in\mathbb{F}_q^\times} \chi'(x)\psi'(x)$$

とする. このとき

定理 2.1. (Davenport and Hasse (1938))

$$-G_q(\chi \circ N_{\mathbb{F}_q/\mathbb{F}_p}, \psi \circ T_{\mathbb{F}_q/\mathbb{F}_p}) = (-G_p(\chi,\psi))^m$$

Lamprecht ([13], 1957) は有限環 R につき次の和を考えることを提唱し基本的な性質を調べた. $\mathbb{F}_p$ の場合と同様に χ を R の可逆元全体のなす乗法群 $R^\times$ の指標, ψ を R の加法的な指標とする.

$$G_R(\chi,\psi) = \sum_{x\in R^\times} \chi(x)\psi(x)$$

後述するように近藤武 ([12], 1963) は $R = M_n(q)$ (= 有限体 $\mathbb{F}_q$ 上の n 次正方行列全体の成す環) の場合にこの和を求めた.

有限群の立場からすると有限環を経由せず次のような和を考えることが自然である.

定義 2.2. G を有限群, $R: G \to GL_n(\mathbb{C})$ を G の通常表現, $\rho: G \to GL_m(\mathbb{F}_q)$ を G のモジュラー表現とする. このとき

$$W_G(R,\rho) = \sum_{x\in G} R(x)\psi(\mathrm{Tr}\ \rho(x))$$

を G 上の R,ρ に付随したガウス和という. ただし, ψ は $\mathbb{F}_q$ の非自明な加法的指標である.

さらに行列 $W_G(R,\rho)$ のトレースを $\tau_G(\chi_R)$ と書く. ここで χ_R は R の指標を表す.

容易に分かるように R が既約のとき $W_G(R,\rho)$ はスカラー行列であり, 従って $W_G(R,\rho) = w(R)I_n$ とすると $\tau_G(\chi_I) = w(R)\deg R$ である.

τ_G は G の Grothendieck 群の指標に自然に拡張ができる.

Kim, Lee, Park らは ([11], 1996) からはじまる一連の仕事において, R が単位表現, G が有限古典群, ρ が G の自然表現の場合に $W_G(1,\rho)=w(R)=\tau_G(\chi_R)$ の値を具体的に求めた.

有限簡約群に話を移す前にガウス和以外の指標和についても準備をする.

3. Kloosterman sums and unitary Kloosterman sums

以後このノートを通して次の記号を使う. $k=\mathbb{F}_q$ は q 元よりなる有限体, k の代数閉体 $\bar{k}$ を一つ固定し $k_m=\mathbb{F}_{q^m}$ を $\bar{k}$ における k の m 次拡大体とする. また C_m を $\bar{k}^\times$ における位数 q^m+1 の巡回群とする. 特に $C=C_1$ とする. ψ は k の非自明な固定された加法的指標で, $\psi^{(m)}=\psi\circ T_{k_M/k}$ は ψ の自然な k_m への持ち上げとする.

π を $k^\times$ の乗法的指標とするとき次の和

$$K(\psi,\pi,a)=\sum_{st=a}\psi(s+t)\pi(s),\ a\in k^\times$$

は, (一般) Kloosterman sum とよばれる. $a=1$ のとき単に $K(\psi,\pi)$ と書く. また φ を C の指標とするとき

$$J(\psi,\varphi)=\sum_{\alpha\in C}\psi(\alpha+\alpha^{-1})\varphi(\alpha)$$

を unitary Kloosterman sum とよぶ [6].

π の k_m への自然な持ち上げを π_m とし,

$$\varphi_m(x)=\begin{cases}\varphi(x^{(1+q^m)/(1+q)}), & m: odd, x\in C_m\\ \varphi(x^{(1-q^m)/(1+q)}), & m: even, x\in k_m\end{cases}$$

により自然な持ち上げ φ_m を定める. 対応する k_m 上, C_m 上の Kloosterman 和, unitary Kloosterman 和をそれぞれ $K_m(\pi_m,a)$, $K_m(\varphi_m)$, $J_m(\varphi_m)$ と略記する.

この指標和に対する Davenport-Hasse 型の定理を記述するため Dickson 多項式 $P_m(u,v)$ を形式的巾級数環 $\mathbb{Z}[u,v][[z]]$ の中で次のように定義する.

$$\frac{uz+2vz^2}{1+uz+vz^2}=\sum_{m\geq 1}P_m(u,v)z^m$$

すると (cf.[2], [6])

定理 3.1.

(1) $$P_m(K(\psi,\pi,a),q\pi(-a))=K_m(\pi_m,a),$$

(2) $$P_m(J(\psi,\varphi),q\varphi(-1)) = \begin{cases} K_m(\varphi_m), & m\ :\ \text{偶数} \\ J_m(\varphi_m), & m\ :\ \text{奇数} \end{cases}$$

$\pi^2=1, \varphi^2=1$ のときは, さらに次の性質が分かっている. (cf. [3],[9], [6])

命題 3.2. 1 を $k^\times$ の自明な指標, π_0 (resp.φ_0) を $k^\times$ (resp. C) の位数 2 の指標とする. このとき

(1) $$J(\psi,1,a) = -K(\psi,1,a),$$

(2) $$K(\psi,\pi_0) = G(\pi_0,\psi)(\psi(2)+\psi(-2)),$$

(3) $$J(\psi,\varphi_0) = G(\pi_0,\psi)(\psi(-2)-\psi(2)).$$

ここで $G(\pi_0,\psi)$ は k 上のガウス和である.

雑記 3.3. 上記 unitary Kloosterman 和の定義と性質は有限線型群のガウス和の考察から必要な物であった. 同時に Gelfand-Graev 表現からも現われる自然な和である. 1997 年に Isaac Newton Institute (Cambridge) で行われたプログラム "Representation Theory of Algebraic Groups and Related Finite Groups" に C. W. Curtis と著者は別々に参加したのだが, 宿に着いて町を散歩しているときに研究所ではなく路上でばったりと出会い, 時候の挨拶のあとで何を考えているかという話になった. そのとき, 今では unitary Kloosterman 和 とよんでいるものを, お互いに別の方向から考えていることが分かり非常に驚いた. それがその後の 2 篇の共著論文につながった ([6], [7]). ただしこのノートでは Gelfand-Graev 表現との関係は論じない.

4. Gaussian sums over finite reductive groups

4.1. **Deligne-Lusztig 一般指標に対応するガウス和.** 前の節のように $k=\mathbb{F}_q$ とする. $\mathbf{G}$ を k 上定義された連結簡約代数群, σ を $\mathbf{G}$ の対応するフロベニウス写像とする. また $G=\mathbf{G}^\sigma$ を σ による $\mathbf{G}$ の固定点のなす有限群, $R: G\to GL_m(\mathbb{C})$ を G の通常表現, ϕ を G 上の $\mathbb{C}$ 値類関数で, $x\in G$ に対し $x=x_sx_u$ をその Jordan 分解とするとき, x_s : 半単純成分, x_u : 巾単成分,

(#) $$\phi(x)=\phi(x_s)$$

が成り立つとする. W_G, w, τ_G を第 2 節のように定める.

σ 不変な $\mathbf{G}$ の極大トーラス $\mathbf{T}$ と $T = \mathbf{T}^\sigma$ の指標, θ, に対して対応する Deligne-Lustzig 一般指標を $R_{\mathbf{T},\theta}$ と書く (cf. [8]).

このとき次が成り立つ (cf.[15]).

定理 4.2.

$$\tau_W(R_{\mathbf{T},\theta}) = \frac{|G|}{|T|}\sum_{t\in T}\theta(t)\phi(t).$$

特に θ が一般の位置にあるとき

$$w(\epsilon_{\mathbf{G}}\epsilon_{\mathbf{T}}R_{\mathbf{T},\theta}) = \epsilon_{\mathbf{G}}\epsilon_{\mathbf{T}}|G|_p\sum_{t\in T}\theta(t)\phi(t).$$

ρ を G の k 上のモジュラ-表現とし, $\psi : k^+ \to \mathbb{C}^\times$, $\psi \neq 1$ を用い

$$\phi(x) = \psi(\mathrm{Tr}\ \rho(x)), \quad x \in G$$

とすると ϕ は上の条件 (#) をみたしている.

4.3. $GL_n(q)$. $\Phi = \{f(t) \in k[t] \mid f(t)$ 既約, monic, $f(0) \neq 0\}$, $\mathcal{P}$ を分割 (partition) 全体の集合とする. $G = GL_n(q)$ の既約指標は

$$\{\lambda \mid \lambda : \Phi \to \mathcal{P}, \sum_{f\in\Phi}|\lambda(f)|\deg f = n\}$$

と 1 対 1 に対応していることが知られている (cf. J.A.Green [10]). λ に対応する G の既約指標を ξ^λ とする.

また ρ は G の自然表現とする. このとき

定理 4.4. (Kondo,[12])

$$w(\xi^\lambda) = (-1)^{n-\sum_{f\in\Phi}|\lambda(f)|}q^{\binom{n}{2}}\prod_{f\in\Phi}G_{\deg f}(\pi_f)^{|\lambda(f)|}$$

ここで π_f は f が定める $k_{\deg f}$ の乗法的指標であり $G_{\deg f}(\pi_f)$ は体 $k_{\deg f}$ 上の乗法的指標 π_f 加法的指標 $\psi^{(\deg f)}$ に対応するガウス和である.

以下では斜交群と例外群 G_2 に対してガウス和がどのような形になるかを Kloosterman 和との関わりの中で見ていく.

4.5. **斜交群.** $\mathbf{G} = \{g \in GL_{2n}(\bar{k}) : J = {}^t gJg\}$, $J = \begin{pmatrix} 0 & 1_n \\ -1_n & 0 \end{pmatrix}$ $\sigma((g_{ij})) = (g_{ij}^q)$ とする. このとき $G = \mathbf{G}^\sigma$ は $2n$ 次の斜交群で $Sp_{2n}(q)$ と書かれる.

$\mathbf{G}$ の σ 不変な極大トーラスの G-共役類は C_n 型ワイル群の共役類, したがって n の double partition $\mathcal{P}_n^{(2)}$, つまり $\mathcal{P}_n^{(2)} = \{(\lambda, \mu) \mid \lambda, \mu \in \mathcal{P}, |\lambda| + |\mu| = n\}$, と 1 対 1 に対応している. ここで $\mathcal{P}$ は分割の集合である.

$\mathbf{T}_{\lambda,\mu}$ を double partition $(\lambda, \mu) \in \mathcal{P}_n^{(2)}$ に対応する極大トーラスとする. ここで $\lambda = (\lambda_1, \ldots, \lambda_r)$, $\mu = (\mu_1, \ldots, \mu_s)$ とする. (λ_i, μ_j はそれぞれ λ, μ の parts である.) $T_{\lambda,\mu} = \mathbf{T}_{\lambda,\mu}^\sigma$ は次の群と同型になる：

$$\prod_{i=1}^{r} k_{\lambda_i}^\times \times \prod_{j=1}^{s} C_{\mu_j}.$$

π_i, φ_j をそれぞれ $k_{\lambda_i}^\times$, C_{μ_j} の指標とし, θ を $((\pi_i), (\varphi_j))$ に上の同型を通して対応する $T_{\lambda,\mu}$ の指標とする.

さらに ρ を G の $GL_{2n}(q)$ 中への自然表現とし $\phi(g) = \psi(\mathrm{Tr}\ g)$, $g \in G$, とする. すると (cf. ([15], Proposition 2.3)

命題 4.6.

$$\tau_W(R_{\mathbf{T}_{\lambda,\mu},\theta}) = |G : T_\lambda| \prod_{i=1}^{r} K_{\lambda_i}(\pi_i) \times \prod_{j=1}^{s} J_{\mu_j}(\varphi_j).$$

特に θ が一般の位置のときは

$$w((-1)^{n+r} R_{\mathbf{T}_{\lambda,\mu},\theta}) = (-1)^{n+r} q^{n^2} \prod_{i=1}^{r} K_{\lambda_i}(\pi_i) \times \prod_{j=1}^{s} J_{\mu_j}(\varphi_j).$$

ここでは述べないがユニタリ群や直交群に対しても同様の命題が成り立つ.

次数が低いときは第 3 節の内容を用いて, 全ての既約表現に対するガウス和を計算することができる.

4.7. $Sp_4(q)$. 以下に $Sp_4(q)$ の既約指標に対するガウス和の表をのせる. 既約指標の記号は B. Srinivasan [17] のものである.

χ_R	$: w(\chi_R)$	
$\chi_1(\varphi')$	$: q^4 J_2(\varphi')$	
$\chi_2(\pi')$	$: q^4 K_2(\pi')$	
$\chi_3(\pi_1, \pi_2)$	$: q^4 K_1(\pi_1) K_1(\pi_2)$	
$\chi_4(\varphi_1, \varphi_2)$	$: q^4 J_1(\varphi_1) J_1(\varphi_2)$	
$\chi_5(\pi, \varphi)$	$: q^4 K_1(\pi) J_1(\varphi)$	
$\chi_6(\varphi)$	$: -q^4 J_1(\varphi)^2$	$+q^5(q+1)\varphi(-1)$
$\chi_7(\varphi)$	$: q^4 J_1(\varphi)^2$	$-q^4(q+1)\varphi(-1)$
$\chi_8(\pi)$	$: q^4 K_1(\pi)^2$	$+q^5(q-1)\pi(-1)$
$\chi_9(\pi)$	$: q^4 K_1(\pi)^2$	$-q^4(q-1)\pi(-1)$
$\xi_1(\varphi), \xi_1'(\varphi)$	$: -q^4 J J_1(\varphi)$	
$\xi_3(\pi), \xi_3'(\pi)$	$: q^4 K K_1(\pi)$	
$\xi_{21}(\varphi), \xi_{22}(\varphi)$	$: q^4 K_1(\pi_0) J_1(\varphi)$	
$\xi_{21}'(\varphi), \xi_{22}'(\varphi)$	$: q^4 J_1(\varphi) J_1(\varphi_0)$	
$\xi_{41}(\pi), \xi_{42}(\pi)$	$: q^4 K_1(\pi) K_1(\pi_0)$	
$\xi_{41}'(\pi), \xi_{42}'(\pi)$	$: q^4 K_1(\pi) J_1(\varphi_0)$	
$\Phi_1, \Phi_2, \Phi_3, \Phi_4$	$: q^4 K J_1(\varphi_0)$	
$\Phi_5, \Phi_6, \Phi_7, \Phi_8$	$: q^4 K K_1(\pi_0)$	
Φ_9	$: q^4 K_1(\pi_0)^2$	$+q^4(q-1)^2\pi_0(-1)$
θ_1, θ_2	$: q^4 K_1(\pi_0)^2$	$-2q^4(q-1)^2\pi_0(-1)$
θ_3, θ_4	$: q^4 K_1(\pi_0)^2$	$+2q^5(q-1)\pi_0(-1)$
$\theta_5, \theta_6, \theta_7, \theta_8$	$: q^4 K_1(\pi_0) J_1(\varphi_0)$	
θ_9	$: q^4 K^2$	$+q^4(q-1)^2$
θ_{10}	$: q^4 K^2$	$-q^4(q+1)^2$
θ_{11}	$: q^4 K^2$	$+q^4(q^2-1)$
θ_{12}	$: q^4 K^2$	$-q^4(q^2-1)$
$\theta_{13} = St$	$: q^4 K^2$	$-q^3(q^2-1)$
$\theta_0 = 1$	$: q^4 K^2$	$+q^5(q^2-1)$

ここで $K = K_1(1), J = J_1(1) = -K$.

4.8. G_2 型 **Chevalley 群.** $\mathbf{G}$ を G_2 型の Chevalley 群とし, ρ を $G = \mathbf{G}^{\sigma}$ の 7 次のモデュラー表現とする. さらに

$$S_1 := \sum_{\substack{x_1, x_2, x_3 \in k \\ x_1 x_2 x_3 = 1}} \psi(x_1 + x_2 + x_3 + x_1^{-1} + x_2^{-1} + x_3^{-1})$$

とする. ここで ψ は k の非自明な加法的指標である. G には 10 個の既約巾単表現が存在する. これらに対応するガウス和は次で与えられる. X_{1_j} は Chang-Ree [4] の記号である.

定理 4.9.

$$
\begin{aligned}
w(X_{11}) &= q^6\psi(1)S_1 + q^7(q^3-1)\psi(-2) + q^7(q^2-1)(q^2+2)\psi(-1),\\
w(X_{12}) &= q^6\psi(1)S_1 - q^4(q^3-1)\psi(-2) - q^3(q^2-1)(2q^2+1)\psi(-1),\\
w(X_{13}) &= q^6\psi(1)S_1 + q^6(q-1)(2q+1)\psi(-2),\\
w(X_{14}) &= q^6\psi(1)S_1 - q^6(q-1)(q+2)\psi(-2),\\
w(X_{15}) &= q^6\psi(1)S_1 + q^6(q-1)^2\psi(-1),\\
w(X_{16}) &= q^6\psi(1)S_1 + 2q^6(q-1)^2\psi(-2) + 3q^6(q-1)^2(q^2+2)\psi(-1),\\
w(X_{17}) &= q^6\psi(1)S_1 - 2q^6\psi(-2) - q^6(q+1)^2\psi(-1),\\
w(X_{18}) &= q^6\psi(1)S_1 + 2q^6(q^2+q+1)\psi(-2) - 3q^6(q+1)^2\psi(-1),\\
w(X_{19}) &= w(\overline{X_{19}})\\
&= q^6\psi(1)S_1 - q^6(q^2+q+1)\psi(-2) - 3q^7\psi(-1).
\end{aligned}
$$

注 4.10. X_{11} は単位表現でありこの場合は既に Lee-Park [14] により求められている.

(4.6), (4.7), (4.9) 等の例をみると有限簡約代数群の既約表現に対応するガウス和は G, K, J, S などの指標和と q の多項式との和となっている. 既約指標とこれらとの間の明示的な対応があるはずで, 分かれば大変におもしろいと思う.

---

10 月のシンポジウム当日は著者の不注意で, お世話をして頂いている諸先生をはじめ皆様に御迷惑をお掛け致しました. お詫び申し上げます.

References

[1] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi sums*, Wiley-Interscience, 1998.

[2] L. Carlitz, Kloosterman sums and finite field extensions, *Acta Arith.*, **16**(1969), 179-193.

[3] B.Chang, Decomposition of the Gelfand-Graev characters of $GL_3(q)$, *Comm. Algebra* **4**(1976), 375-401.

[4] B.Chang and R.Ree, The characters of $G_2(q)$, *Ist. Naz. di Alta Mat., Symposia Mathematica XIII, Academic Press, London* (1974), 395-413.

[5] C. W. Curtis, On the Gelfand-Graev representations of a reductive group over a finite field, *J. Algebra* **157**(1993), 517-533.

[6] C. W. Curtis and K. Shinoda, Unitary Kloosterman sums and Gelfand-Graev representation of GL_2, *J. Algebra* **216**(1999), 431-447.

[7] C. W. Curtis and K. Shinoda, Zeta functions and functional equations associated with the components of the Gelfand-Graev representations of a finite reductive group, Advanced Studies in Pure Math. **40** (2004), 121 – 139.

[8] P. Deligne and G. Lusztig, Representations of reductive groups over finite fields, *Ann. of Math.*, **103**(1976), 103-161.

[9] R. J. Evans, Hermite character sums, *Pacific J. Math.*, **122**(1986), 357-390.

[10] J. A. Green, The characters of the finite general linear groups, *Trans. Amer. Math. Soc.*, **80** (1955), 402-447.

[11] D. S. Kim and I. Lee, Gauss sums for $O^+(2n,q)$, *Acta Arith.*, **78**(1996), 75-89.

[12] T. Kondo, On Gaussian sums attached to the general linear groups over finite fields, *J. Math. Soc. Japan*, **15**(1963), 244-255.

[13] E. Lamprecht, Structure und Relationen allgemeiner Gausscher Summen in endlichen Ringen I,II, *J. Reine Angew. Math.*, **197**(1957), 1-48.

[14] I. Lee and K. Park, Gauss sums for $G_2(q)$, *Bull. Korean Math. Soc.*, **34**(1997), 305-315.

[15] N. Saito and K. Shinoda, Character Sums Attached to Finite Reductive Groups, *Tokyo J. Math.* 23(2000), 373-385.

[16] N. Saito and K. Shinoda, Some character sums and Gauss sums over $G_2(q)$, *Tokyo J. Math.* **24** (2001), 277 – 289.

[17] B. Srinivasan, The characters of the finite symplectic group $Sp(4,q)$, *Trans. Amer. Math. Soc.*, **131**(1968), 488-525.