ガウス和、ヤコビ和そして指標和

寺杣友秀

1. 序

有限体の代数幾何学について古典的な指標和から導入し、現代数学で使われているホモロジー的手法について紹介する。現在では数論と代数幾何の交錯する分野となっている。

2. ガンマ関数、ベータ関数の有限体での類似

2.1. **ガウス和.**

2.1.1. ガンマ関数、ベータ関数の有限体での類似物についてのべる。

$$\Gamma(s) = \int_0^\infty e^{-x} x^s \frac{dx}{x}$$

と書くと、e^x は $\mathbf{R}_+$ 上の加法的な指標、x^s は $\mathbf{R}_+^\times$ の乗法的な指標、$\frac{dx}{x}$ は乗法的な群の作用による不変測度とみなせる。その有限体上の類似物を定義したい。それはガウス和と呼ばれる。

$\mathbf{F}_q$ を有限体、$\chi : \mathbf{F}_q^\times \to \mathbf{C}^\times$ を乗法群の指標、$\psi : \mathbf{F}_q \to \mathbf{C}^\times$ を非自明な加法的な指標とする。このとき

$$G(\chi, \psi) = \sum_{x \in \mathbf{F}_q^\times} \chi(x)\psi(x)$$

と定義する。さらに χ が非自明であるとする。

2.1.2. e^{-x} という関数は標準的な加法指標である。ψ の取り換えについて。$\psi(x)$ を $\psi'(x) = \psi(tx)$ $(t \in \mathbf{F}_q^\times)$ で取り替えてみる。

$$\begin{aligned} G(\chi, \psi') &= \sum_{x \in \mathbf{F}_q^\times} \chi(x)\psi(tx) \\ &= \sum_{x \in \mathbf{F}_q^\times} \chi(t^{-1}x)\psi(x) \\ &= \chi(t^{-1})G(\chi, \psi) \end{aligned}$$

1 のべき根の違いしかでない。従って絶対値には意味があるはず。以下の計算で乗法指標については 0 における値を 0 であるとして定義域を延長しておく。

2.1.3. $G(\chi,\psi)$ の絶対値を求めてみよう。

$$\begin{aligned}
G(\chi,\psi)\overline{G(\chi,\psi)} &= G(\chi,\psi)G(\chi^{-1},\psi^{-1}) \\
&= \sum_{x\in\mathbf{F}_q, y\in\mathbf{F}_q^\times} \chi(xy^{-1})\psi(x-y) \\
&= \sum_{t\in\mathbf{F}_q, y\in\mathbf{F}_q^\times} \chi(t)\psi(ty-y) \\
&= \chi(1)(q-1) + \sum_{t\in\mathbf{F}_q-\{1\}, y\in\mathbf{F}_q^\times} \chi(t)\psi((t-1)y) \\
&= (q-1) - \sum_{t\in\mathbf{F}_q-\{1\}} \chi(t) = q
\end{aligned}$$

従って $|\, G(\chi,\psi)\,| = \sqrt{q}$ となる。

2.2. ヤコビ和.

2.2.1. つぎにベータ関数の有限体の類似物を考えてみよう。

$$B(s,t) = \int_0^1 x^{s-1}(1-x)^{t-1}dx$$

ガンマ関数のときと同様に考える。χ,φ を $\mathbf{F}_q^\times$ の乗法的な指標として、ヤコビ和を次の式で定義する。

$$J(\chi,\varphi) = \sum_{x\in\mathbf{F}-\{0,1\}} \chi(x)\varphi(1-x) = \sum_{x+y=1} \chi(x)\varphi(y)$$

2.2.2. ガンマ関数、ベータ関数の間には次のような関係式がある。

$$B(s,t) = \frac{\Gamma(s)\Gamma(t)}{\Gamma(s+t)}$$

じつはガウス和とヤコビ和にも同様の関係式があることが示せる。$\chi,\varphi,\chi\varphi$ が非自明であるとして、

$$\begin{aligned}
G(\chi,\psi)G(\varphi,\psi) &= \sum_{x,y\in\mathbf{F}_q} \chi(x)\varphi(y)\psi(x+y) \\
&= \sum_{t\in\mathbf{F}_q} \psi(t) \sum_{x+y=t} \chi(x)\varphi(y) \\
&= \sum_{x+y=0} \chi(x)\varphi(y) + \sum_{t\in\mathbf{F}_q^\times} \psi(t) \sum_{x+y=t} \chi(x)\varphi(y) \\
&= \sum_{t\in\mathbf{F}_q^\times} \psi(t) \sum_{\xi+\eta=1} \chi(t\xi)\varphi(t\eta) \\
&= G(\chi\varphi,\psi)J(\chi,\varphi)
\end{aligned}$$

となり従って

$$J(\chi,\varphi)=\frac{G(\chi,\psi)G(\varphi,\psi)}{G(\chi\varphi,\psi)}$$

を得る。とくに $\mid J(\chi,\varphi)\mid=\sqrt{q}$.

3. フェルマー曲線の周期積分と点の個数

3.1. **周期積分.**

3.1.1. 複素数体上の射影平面内の非特異曲線

$$C=\{(x:y:z)\in\mathbf{P}^2_{\mathbf{C}}\mid X^d+Y^d=Z^d\}$$

はフェルマー曲線とよばれる。これの曲線には $(\zeta_1,\zeta_2,\zeta_3)\in\mu_d\times\mu_d\times\mu_d$ が作用するが、対角型 (ζ,ζ,ζ) は自明に作用する。従って

$$G=(\mu_d\times\mu_d\times\mu_d)/\{(\zeta,\zeta,\zeta)\}$$

が作用する。

3.1.2. C の二つのコホモロジー理論、特異コホモロジー $H^1_B(C,\mathbf{Q})$ とドラム・コホモロジー $H^1_{dR}(C,\mathbf{C})$ およびその間の de Rham の定理による同型

$$\begin{aligned}H^1_{dR}(C,\mathbf{C})&\simeq H^1_B(C,\mathbf{Q})\otimes\mathbf{C}\\&=Hom(H_1(C,\mathbf{Q}),\mathbf{C})\end{aligned}$$

を考える。これらの同型は G の作用と compatible である。

3.1.3. C から無限遠直線 $\{Z=0\}$ との交点を除いて、非斉次座標 $x=X/Z, y=Y/Z$ を用いて表すと $x^n+y^n=1$ となる。$H^1_{dR}(C,\mathbf{C})$ において、G の作用の固有空間の基底として

$$\eta_{a,b}=t^{\frac{a}{d}-1}(1-t)^{\frac{b}{d}-1}dt$$

がとれる。$0<a<d, 0<b<d, a+d\neq d$ を動き、$t=x^n$ と変数変換して $x=t^{\frac{1}{d}}, y=(1-t)^{\frac{1}{d}}$ と分枝をとった。$a+d<d$ のときは正則微分で $a+d>d$ のときは有理微分だが、$H^1_{dR}(C,\mathbf{C})$ の元を定めている。

3.1.4. $H_1(C,\mathbf{Q})$ は $\mathbf{Q}[G]$-加群として次のポッホハマーサイクル

$$\gamma=\rho_0\rho_1\rho_0^{-1}\rho_1^{-1}$$

で生成される。γ と $\eta_{a,b}$ のペアリングは積分で与えられるので、

$$\int_\gamma\eta_{a,b}=(1-\mathbf{e}(\frac{a}{d}))(1-\mathbf{e}(\frac{b}{d}))B(\frac{a}{d},\frac{b}{d})$$

3.1.5. じつは $H_{dR}(C)$ には $\mathbf{Q}$ 上のベクトル空間の構造がはいる。つまり $\mathbf{Q}$ 上に定義された微分形式というのが well defined になる。これは C が代数多様体であるということを使って導入される構造である。二つの $\mathbf{Q}$ 構造の変換行列には $B(s,t)$ の形の超越的な数が現れる。ここに現れる積分を周期積分という。

3.2. **フェルマー曲線の点の個数とヤコビ和.**

3.2.1. $\mathbf{F}_q$ を有限体、フェルマー曲線の次数 d は $q-1$ を割り切るとする。フェルマー曲線の解集合の個数をもとめる。

$$N_{aff} = \#\{(x,y) \in \mathbf{F}_q \times \mathbf{F}_q \mid x^d + y^d = 1\}$$

とおく。μ_d を $\mathbf{C}^\times$ の 1 の d 乗根の全体のなす群とする。群準同型 $H = Hom(\mathbf{F}_q^\times, \mu_d)$ のなす群の生成元をひとつ固定して $\mathbf{Z}/d\mathbf{Z}$ をと同一視する。$t \in \mathbf{F}_q^\times$ に対して

$$\#\{x \mid x^d = t\} = \sum_{\chi \in H} \chi(t)$$

という等式を用いて解の数を数える。

3.2.2. まずは $x^d \neq 0, 1$ の部分の個数 N_0 をもとめよう。このとき $y^d \neq 0, 1$ となる。従って

$$\begin{aligned} N_0 &= \sum_{x \neq 0,1} \sum_{\chi, \varphi \in H} \chi(x)\varphi(1-x) \\ &= \sum_{\chi, \varphi \in H} \sum_{x \neq 0,1} \chi(x)\varphi(1-x) \end{aligned}$$

最後の和の形で $\chi, \varphi, \chi\varphi$ が非自明な時はヤコビ和で表されるから、そうでない項を計算する。

(1) $\chi = 1, \varphi \neq 1$ の時。(あるいは $\chi \neq 1, \varphi = 1$ の時。)

$$\sum_{x \neq 0,1} \varphi(1-x) = -\varphi(1) = -1$$

このような (χ, φ) の組み合わせは $2d-2$ 個ある。

(2) $\chi = \varphi = 1$ の時。$\sum_{x \neq 0,1} 1 = q-2$

(3) $\chi = \varphi^{-1} \neq 1$ の時。

$$\sum_{x \neq 0,1} \chi(x/(1-x)) = -\chi(-1)$$

3.2.3. $x = 0, 1$ の部分も合わせて、ヤコビ和以外の部分は

$$-(2d-2) + q - 2 - \sum_{\chi \neq 1} \chi(-1) + \underbrace{2d}_{x=0,1} = q + 1 - \sum_{\chi \in H} \chi(-1)$$

また $X^d + Y^d = Z^d$ を考えたとき無限遠直線 $Z = 0$ との交点の個数 N_∞ は

$$\#\{(X/Y)^d = -1\} = \sum_{\chi \in H} \chi(-1)$$

となるので

$$\begin{aligned} N &= \#\{(X:Y:Z) \in \mathbf{P}^2(\mathbf{F}_q) \mid X^d + Y^d = Z^d\} \\ &= N_{aff} + N_\infty \\ &= q + 1 + \sum_{\substack{\chi \neq 1, \varphi \neq 1, \\ \chi\varphi \neq 1}} J(\chi, \varphi) \end{aligned}$$

4. Lefschetz の不動点公式

4.1. **向き付け可能コンパクトな可微分多様体の場合.** 周期積分がコホモロジーの言葉で記述できたように解の個数もコホモロジーのことばで記述できる。まずは位相空間における Lefschetz の不動点公式を述べよう。

4.1.1. M を向き付け可能コンパクト n 次元可微分多様体とする。$f : M \to M$ を自分自身への可微分写像として、f の不動点集合 $\Sigma = \{x \in M \mid f(x) = x\}$ が有限離散集合であるとする。さらに Σ の各点 x において f の微分 Tf_x は 1 を固有値を持たないとする。

4.1.2. このとき次の定理が成り立つ。

定理 4.1. (1) 不動点の x の符号 $\mathrm{sgn}(x)$ が Tf_x によって定まる。
(2) 不動点公式

$$\sum_{x\in\Sigma} \mathrm{sgn}(x) = \sum_{i=1}^{n} (-1)^i \,\mathrm{trace}(f^*; H^i(M, \mathbf{Q}))$$

Proof. 不動点の個数 (符号付き) を対角部分 $\Delta = \{(x, x) \in M \times M \mid x \in M\}$ と f のグラフ Γ_f の交点 (符号付き) として求める。対角成分の $H^n(M \times M, \mathbf{Q})$ におけるコホモロジー類は Kunneth 分解して、

$$\Delta = \Delta_0 + \cdots + \Delta_n \in (H^0(M, \mathbf{Q}) \otimes H^n(M, \mathbf{Q})) \oplus \cdots \oplus (H^n(M, \mathbf{Q}) \otimes H^0(M, \mathbf{Q}))$$

Poincare 双対定理を用いて

$$H^{n-i}(M, \mathbf{Q}) \otimes H^i(M, \mathbf{Q}) \simeq Hom(H^i(M, \mathbf{Q}), H^i(M, \mathbf{Q}))$$

なる同型を得るが、Δ の成分 Δ_{n-i} は id に対応する。従って $v_1^{(i)}, \ldots, v_{b_i}^{(i)}$ を $H^i(M, \mathbf{Q})$ の基底、$v_1^{(i)*}, \ldots, v_{b_i}^{(i)*}$ を $H^{n-i}(M, \mathbf{Q})$ における Poincare 双対基底とすると、

$$\Delta_{n-i} = \sum_j v_j^{(i)*} \otimes v_j^{(i)},$$

となり、Γ_f の $H^i(M, \mathbf{Q}) \otimes H^{n-i}(M, \mathbf{Q})$ 成分 $\Gamma_{f,i}$ は

$$\Gamma_{f,i} = \sum_j f^* v_j^{(i)} \otimes v_j^{(i)*},$$

となる。従って

$$\Delta_{n-i} \cdot \Gamma_{f,i} = (-1)^i \,\mathrm{trace}(f^*; H^i(M, \mathbf{Q}))$$

となり、定理が示される。 □

4.2. **Etale cohomology.**

4.2.1. $\mathbf{F}_q$ 上の代数多様体上のよい cohomology 理論がグロタンディークの始めた etale cohomology の理論である。上の Lefschetz の不動点定理を導く際に必要であったコホモロジーの有限次元性、Kunneth の公式、Poincare duality, サイクル写像と intersection 理論が実際に成立する。Lefschetz の不動点定理はその帰結といえる。

4.2.2. $\overline{X}$ を $\mathbf{F}_q$ 上に定義された代数多様体 X を $\mathbf{F}_q$ の代数的閉包 $\overline{\mathbf{F}_q}$ 上で考えたものとする。

C をフェルマー曲線として、その非斉次座標を (x,y) と書く。このとき $F: C \to C$ を $(x,y) \to (x^q, y^q)$ で定義された代数多様体の写像とする。これを相対フロベニウス写像という。この写像は $\mathbf{F}_q$ 上定義されているので $\overline{\mathbf{F}_q}$ 上の写像に延長される。

$\overline{C}$ の i 次 l 進 etale cohomology を $H^i_{et}(\overline{C}, \mathbf{Q}_l)$ と書く。このとき写像 F は $F^*: H^i(\overline{C}, \mathbf{Q}_l) \to H^i(\overline{C}, \mathbf{Q}_l)$ なる写像を引き起こす。

命題 4.2. (1) フロベニウス写像の固定点の個数は C の $\mathbf{F}_q$ に座標を持つ点の個数 N と等しい。

(2) それぞれのコホモロジーにおけるトレースは以下のとおり。

$$\begin{aligned}
&\mathrm{trace}(F^*; H^0(\overline{C}, \mathbf{Q}_l)) = 1 \\
&\mathrm{trace}(F^*; H^1(\overline{C}, \mathbf{Q}_l)) = -\sum_{\substack{\chi\neq 1, \varphi\neq 1, \\ \chi\varphi\neq 1}} J(\chi,\varphi) \\
&\mathrm{trace}(F^*; H^2(\overline{C}, \mathbf{Q}_l)) = q
\end{aligned}$$

さらに強く、$-J(\chi,\varphi)$ $(\chi \neq 1, \varphi \neq 1, \chi\varphi \neq 1)$ は F^* の $H^1(\overline{C}, \mathbf{Q}_l)$ の固有値である。

(3) $\chi \neq 1, \varphi \neq 1, \chi\varphi \neq 1$ のもとで $\mid J(\chi,\varphi) \mid = \sqrt{q}$.

4.2.3. 最後の絶対値の公式は Riemann 予想の類似といわれていて、$\mathbf{F}_q$ 上の完備非特異代数多様体の場合にも予想されていた。これは Weil 予想とよばれ、Deligne により解決された。もう少し超幾何関数などに関連する指標和についても述べたかったが、時間も限られているので、ここではふれない。

5. Appendix

5.1. **Hasse-Davenport の定理.** $\mathbf{F}_{q^e}$ におけるガウス和と $\mathbf{F}_q$ におけるガウス和の関係に関する定理。$\chi: \mathbf{F}^\times \to \mathbf{C}^\times$,$\psi: \mathbf{F}_q \to \mathbf{C}^\times$ を非自明な指標とする。

定理 5.1. $\chi_e = \chi \circ Nm: \mathbf{F}_{q^e}^\times \to \mathbf{F}_q^\times \to \mathbf{C}^\times$, $\psi_e = \psi \circ Tr: \mathbf{F}_{q^e} \to \mathbf{F}_q \to \mathbf{C}^\times$ とおく。このとき、

$$-G(\chi_e, \psi_e) = (-G(\chi,\varphi))^e$$

が成り立つ。

Proof. 以下は Weil の論文にある、なかなか含蓄の深い証明。$\mathbf{F}_q[x]$ の monic polynomial $f(x) = x^d + a_1 x^{d-1} + \cdots + a_d$ に対して $S(f) = \psi(a_1)\varphi(a_d)$ とおく。このとき $S(fg) = S(f)S(g)$ が成り立つので、$\mathbf{F}_q[x]$ の素因子分解の一意性

により

$$\sum_{f:\text{ monic}} S(f)t^{\deg(f)} = \prod_{f:\text{ irred.}} \sum_{i=0}^{\infty} (S(f)t^{\deg(f)})^i$$
$$= \prod_{f:\text{ irred.}} \frac{1}{1 - S(f)t^{\deg(f)}}$$

他方 $a_2, \ldots, a_n$ を固定したとき $\sum_{a_1} \psi(a_1) = 0$ なので左辺の和における 2 次以上の次数の項は 0 となる。従って左辺は $1 + G(\chi, \psi)t$ となる。また

$$G(\chi_e, \psi_e) = \sum_{h|e} \sum_{\substack{f:\text{irred.},\\ \deg(f)=h}} S(f)^{e/h} \cdot h$$

となることに気をつけよう。上の式の両辺の log をとり、

$$\sum_{l=1}^{\infty} (-1)^{l+1} \frac{G(\chi, \psi)^l t^l}{l} = \log(1 + G(\chi, \psi)t)$$
$$= -\sum_{f:\text{irrd.}} \log(1 - S(f)t^{\deg(f)})$$
$$= \sum_{f:\text{irrd.}} \sum_{m=1}^{\infty} \frac{S(f)^m t^{m \deg(f)}}{m}$$
$$= \sum_{l=1}^{\infty} \sum_{\substack{f:\text{irrd.},\\ \deg(f)|l}} \frac{S(f)^{l/\deg(f)} \deg(f)}{l} t^l$$
$$= \sum_{l=1}^{\infty} \frac{G(\chi_l, \psi_l)}{l} t^l$$

これより定理を得る。 □

Remark 5.2. *etale* コホモロジーとそのベッチ数の計算を使えば、もっと容易に証明できる。

この定理から次の二つの系を得る。

系 5.3. $-J(\chi_e, \varphi_e) = (-J(\chi, \varphi))^e$

系 5.4. C の $\mathbf{F}_{q^e}$ に座標を持つ点の個数 N_e は

$$N_e = q^e + 1 - \sum_{\substack{\chi \neq 1, \varphi \neq 1,\\ \chi\varphi \neq 1}} (-J(\chi, \varphi))^e$$

で与えられる。