結び目と素数 – 数論的位相幾何学入門

森下 昌紀 (仙台シンポジウム, 2011.8.25.)

結び目と素数の類似に基づき, 結び目理論 (3 次元トポロジー) と数論の間には親密な類似性がみられる. この類似性に従い, トポロジーと数論の間に橋を架け, お互いに刺激しあって研究しようという領域を数論的位相幾何学と呼ぶ. この講義では, 数論的位相幾何学における基本的な類似を説明し, Gauss から分かれたこの 2 つの道を統一的に眺め直したいと思う.

Gauss の結び目理論は古典電磁気学の中から生まれたが, 結び目理論と数論の関係も現代の場の理論と繋がって行くように思われる.

1. Gauss

• 平方剰余の数論 (Disquisitiones Arithmeticae, 1801)

$\longrightarrow$ 現代の代数的数論へ発展.

奇素数 p と p で割り切れない整数 a に対し, 2 次の合同式

$$x^2 \equiv a \bmod p$$

を考える. この合同式が整数解をもつか否かに従い, a は p を法として平方剰余ないし平方非剰余と呼ばれ, 平方剰余記号が

$$\left(\frac{a}{p}\right) := \begin{cases} +1, & a \text{ は } p \text{ を法として平方剰余}, \\ -1, & a \text{ は } p \text{ を法として平方非剰余} \end{cases}$$

により定義される.

<u>例</u> $x^2 \equiv 5 \bmod 17$ をみたす $x = 1, \ldots, 16$ はない. $\therefore \left(\frac{5}{17}\right) = -1$.

Gauss は, 2 つの奇素数 p, q に対し, p が q を法として平方剰余であることと q が p を法として平方剰余であることの間には精密な相互関係が成り立つことを証明した (Gauss 相互律):

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

特に, p または $q \equiv 1 \bmod 4$ のときは, 次の対称性が成り立つ:

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right).$$

<u>例</u> $\left(\frac{5}{17}\right) = \left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) = -1$. 相互律により易しい問題 $x^2 \equiv 2 \bmod 5$ に変換される.

Gauss は相互律に 7 つの異なる証明を与えた. その中で, 最も含蓄のある方法の一つは, 等式

$$\left(\frac{q^*}{p}\right) = \left(\sum_{x \in \mathbb{F}_q} \zeta_q^{x^2}\right)^{p-1} \quad \left(\begin{array}{c} q^* = (-1)^{\frac{q-1}{2}} q, \\ \zeta_q = \sqrt[q]{1} \in \overline{\mathbb{F}}_p \end{array}\right).$$

を使うものである. この右辺 (の括弧内) は Gauss 和と呼ばれる.

• 電磁気学 (Zur mathematischen Theorie der electrodynamischen Wirkungen, 1833) $\longrightarrow$ 現代の結び目理論へ発展

K, L を 3 次元 Euclid 空間 $\mathbb{R}^3$ 内の交わらない 2 つのなめらかから有向単純閉曲線とし, そのパラメーター表示を各々 $a : [0,1] \longrightarrow \mathbb{R}^3$, $b : [0,1] \longrightarrow \mathbb{R}^3$ とする. L にその向きに大きさ I の電流を流すとき, 磁場 $\mathbf{B}(x)$ $(x \in \mathbb{R}^3)$ が発生する. Biot-Savart の法則により, $\mathbf{B}(x)$ は次式で与えられる:

$$\mathbf{B}(x) = \frac{I\mu_0}{4\pi} \int_0^1 \frac{b'(t) \times (x - b(t))}{||x - b(t)||^3} dt \quad (\mu_0 : \text{ 真空の透磁率})$$

Gauss が示した積分公式は, $(I\mu_0)^{-1}\mathbf{B}(x)$ を K に沿って線積分するとある整数 $\mathrm{lk}(L, K)$ になる, というものである:

$$\frac{1}{I\mu_0} \int_0^1 \mathbf{B}(a(s)) \cdot a'(s) ds = \mathrm{lk}(L, K),$$

すなわち,

$$\frac{1}{4\pi} \int_0^1 \frac{(b'(t) \times (a(s) - b(t))) \cdot a'(s)}{||a(s) - b(t)||^3} dsdt = \mathrm{lk}(L, K).$$

整数 $\mathrm{lk}(L, K)$ は, K と L の絡み具合を表す量で, まつわり数と呼ばれ, 次のように定義される: まず, L を境界とする曲面を Σ_L とし, Σ_L には L

の向きと同調する向きを与える. K と Σ_L の各交点 P での交わり方は, P での K の接線ベクトルと Σ_L の法線ベクトルが同じ向きか逆向きかのいずれかである. 前者の場合, $\varepsilon(P) := 1$, 後者の場合, $\varepsilon(P) := -1$ と定める. K と Σ_L との交点を $P_1, \ldots, P_m$ とするとき,

$$\mathrm{lk}(L, K) := \sum_{i=1}^{m} \varepsilon(P_i)$$

と定義される.

まつわり数 $\mathrm{lk}(L, K)$ は K, L を連続変形しても変わらない位相不変量の最初の例である.

2. 辞書

トポロジーにおいて, 空間の位相的な形を代数的な言葉で記述する理論として (コ) ホモロジー論, ホモトピー論がある. 数論においても, スキームのエタール位相的な形を記述する理論として, エタール (コ) ホモロジー論, エタールホモトピー論がある.

トポロジー	数論
ホモロジー論	エタールホモロジー論
ホモトピー論	エタールホモトピー論

結び目と素数の類似はこのホモトピー的な視点に基づく.

<u>円周と有限体</u>

円周 $S^1 = K(\mathbb{Z}, 1)$	有限体 $\mathrm{Spec}(\mathbb{F}_q) = K(\hat{\mathbb{Z}}, 1)$
$\pi_1(S^1) = \mathrm{Gal}(\mathbb{R}/S^1) = \langle l \rangle$ l : 1 回りするループ	$\pi_1(\mathrm{Spec}(\mathbb{F}_q)) = \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) = \langle \sigma \rangle$ σ : Frobenius 自己同型

<u>管状近傍と $\mathfrak{p}$-進整数環</u>

管状近傍 V	$\mathfrak{p}$ 進整数環 $\mathrm{Spec}(\mathcal{O}_\mathfrak{p})$
境界 ∂V	$\mathfrak{p}$ 進体 $\mathrm{Spec}(k_\mathfrak{p})$
$1 \to \langle\alpha\rangle \to \pi_1(\partial V) \to \langle\beta\rangle \to 1$ β ：ロンジチュード α：メリディアン $\pi_1(\partial V) = \langle\alpha, \beta \vert [\alpha, \beta] = 1\rangle$	$1 \to I_{k_\mathfrak{p}} \to \pi_1(\mathrm{Spec}(k_\mathfrak{p})) \to \langle\sigma\rangle \to 1$ σ：Frobenius 自己同型 τ：モノドロミー ($\in I_{k_\mathfrak{p}}$ の商) $\pi_1^{\mathrm{tame}}(\mathrm{Spec}(k_\mathfrak{p})) = \langle\tau, \sigma \vert \tau^{q-1}[\tau, \sigma] = 1\rangle$

3次元多様体と代数体の整数環

3次元多様体 M エンド E_M	有限次代数体 k の整数環 $\mathrm{Spec}(\mathcal{O}_k)$ 無限素点の集合 S_k^∞
$S^3 = \mathbb{R}^3 \cup \{\infty\}$	$\mathrm{Spec}(\mathbb{Z}) \cup \{\infty\}$

結び目と素イデアル

結び目 $S^1 \hookrightarrow M$ $S^1 \hookrightarrow \mathbb{R}^3$	素イデアル $\mathrm{Spec}(\mathbb{F}_\mathfrak{p}) \hookrightarrow \mathrm{Spec}(\mathcal{O}_k)$ $\mathrm{Spec}(\mathbb{F}_p) \hookrightarrow \mathrm{Spec}(\mathbb{Z})$
結び目群 $G_K = \pi_1(M \setminus K)$	素イデアル群 $G_{\{\mathfrak{p}\}} = \pi_1(\mathrm{Spec}(\mathcal{O}_k) \setminus \{\mathfrak{p}\})$
ペリフェラル群 D_K $I_K = \langle$ メリディアンの像 $\rangle$	$\mathfrak{p}$ 上の分解群 $D_{\{\mathfrak{p}\}}$ $\mathfrak{p}$ 上の惰性群 $I_{\{\mathfrak{p}\}}$
絡み目 $L = K_1 \cup \cdots \cup K_r$	素イデアルの有限集合 $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$
絡み目群 $G_L = \pi_1(M \setminus L)$	$G_S = \pi_1(\mathrm{Spec}(\mathcal{O}_k) \setminus S)$

ホモロジー群とイデアル類群

$C_2(M) \to Z_1(M)$ $D \mapsto \partial D$	$k^\times \to I(k)$ $a \mapsto (a)$
$B_1(M) = \{\partial D \,\vert\, D \in C_2(M)\}$	$P(k) = \{(a) \,\vert\, a \in k^\times\}$
1次元ホモロジー群 $H_1(M) = Z_1(M)/B_1(M)$	イデアル類群 $H(k) = I(k)/P(k)$
2次元ホモロジー群 $H_2(M)$	単数群 $\mathcal{O}_k^\times$

注　我々の類似はホモトピー的な視点によるが, “円周” $\mathrm{Spec}(\mathbb{F}_p)$ に “長さ” $\log p$ を与えると, 対応する幾何的な対象は 3 次元 Riemann 多様体内の素な閉測地線となる. この方向では, Selberg, 砂田利一, Deninger らにより研究されてきた解析的数論と微分幾何学の類似と合流する.

3. Gauss のまつわり数と平方剰余再論

上の辞書に基づき, Gauss のまつわり数と平方剰余を統一的な視点で見直す.

• まつわり数　$K \cup L \subset \mathbb{R}^3$: 2 成分絡み目.
$Y_K \to X_K = \mathbb{R}^3 \setminus K$: 2 重被覆.

$$\begin{array}{ccc} \pi_1(X_K) & \longrightarrow & \mathrm{Gal}(Y_K/X_K) = \mathbb{Z}/2\mathbb{Z} \\ L & \mapsto & \mathrm{lk}(K,L) \bmod 2. \end{array}$$

• 平方剰余記号　$\{p,q\} \subset \mathrm{Spec}(\mathbb{Z})$: 相異なる 2 奇素数.
$Y_p \to X_p = \mathrm{Spec}(\mathbb{Z}) \setminus \{p\}$: 2 重エタール被覆.
(注: X_p 上に 2 重エタール被覆 (無限素点も不分岐とする) が存在する条件は $p \equiv 1 \bmod 4$. 以下, これを仮定する). Y_p は 2 次拡大 $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ に対応する.

$$\begin{array}{ccc} \pi_1(X_p) & \longrightarrow & \mathrm{Gal}(Y_p/X_p) = \{\pm 1\} \\ \sigma_q & \mapsto & \left(\frac{p}{q}\right). \end{array}$$

◎ まつわり数の対称性と Gauss 相互律が対応している.
◎ まつわり数の Gauss 積分表示のゲージ理論版 (A. Schwarz):

$$\mathrm{lk}(K,L) = \int \mathcal{D}A \exp\left(-\frac{i}{4\pi}\int_{\mathbb{R}^3} A \wedge dA\right) \int_K A \int_L A.$$

ここで, $\int \mathcal{D}A$ は $\mathbb{R}^3$ 上の 1-形式 A にわたる経路積分を表し, Gauss 積分 $\int_{\mathbb{R}} \exp(-x^2)dx$ の無限次元版である. 従って, この積分公式は, 平方剰余記号の Gauss 和による表示の類似とみられる.

まつわり数 $\mathrm{lk}(K,L)$	平方剰余記号 $\left(\frac{q}{p}\right)$
$\mathrm{lk}(K,L) = \mathrm{lk}(L,K)$	$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$
Gauss 積分	Gauss 和

4. 高次まつわり数と多重べき剰余

$L = K_1 \cup \cdots \cup K_n \subset S^3$: n 成分絡み目
$\rightsquigarrow \mu(i_1 \cdots i_r) \in \mathbb{Z}$: 高次まつわり数 (Milnor) s.t. $\mu(ij) = \mathrm{lk}(K_i, K_j)$.

<u>例</u>　ボロミアン環

に対し, $\mu(ij) = 0\ \forall i \neq j,\ \mu(123) = 1$.

$\mu(i_1 \cdots i_r)$ の定義:　$G_L = \pi_1(S^3 \setminus L) = G_L^{(1)} \supset G_L^{(2)} = [G_L, G_L] \supset \cdots \supset G_L^{(n)} = [G_L, G_L^{(n-1)}] \supset \cdots$. このとき, Milnor の表示

$$G_L/G_L^{(n)} = \langle x_1, \ldots, x_n \mid [x_1, y_1] = \cdots = [x_n, y_n] = 1, F^{(n)} = 1 \rangle$$

がある. ここで x_i, y_i は各々K_i のメリディアン, ロンジチュードを表す語, $F = \langle x_1, \ldots, x_n \rangle$ (自由群). このとき, y_j を x_i たちで Magnus 展開したときの係数が高次まつわり数:

$$y_j = 1 + \sum \mu(i_1 \cdots i_r j) X_{i_1} \cdots X_{i_r} \quad (x_i = 1 + X_i)$$

• <u>応用</u> (トポロジー $\rightarrow$ 数論)
$S = \{p_1, \ldots, p_n\}$: n ケの奇素数. G_L と Galois 群 G_S の類似を使い,
$\rightsquigarrow \mu_2(i_1 \cdots i_r) \in \mathbb{F}_2$: 数論的高次まつわり数 (Morishita).

◎ $\mu_2(12 \cdots r)$ の数論的な意味:
「$p_1, \ldots, p_{r-1}$ のみが分岐するある $2^{n(n-1)/2}$ 次 Galois 拡大 $k_r/\mathbb{Q}$ s.t.

$$\mathrm{Gal}(k_r/\mathbb{Q}) = \begin{pmatrix} 1 & \mathbb{F}_2 & \cdots & \cdots & \mathbb{F}_2 \\ & 1 & \mathbb{F}_2 & \cdots & \mathbb{F}_2 \\ & & \ddots & \ddots & \vdots \\ & \text{\huge 0} & & 1 & \mathbb{F}_2 \\ & & & & 1 \end{pmatrix},$$

における p_r の分解の仕方を記述する」

<u>問題</u>　k_r と $\mu_2(12\cdots r)$ の具体的記述.

・ $k_2 = \mathbb{Q}(\sqrt{p_1})$

$$(-1)^{\mu_2(12)} = \left(\frac{p_1}{p_2}\right).$$

・ $k_3 =$ Rédei の 8 次 2 面体拡大 (1939)

$$(-1)^{\mu_2(123)} = [p_1, p_2, p_3]\ (\text{Rédei のトリプル記号}).$$

<u>定理</u> (天野郁弥, 2010)　k_4(64 次拡大) の具体的構成と 4 重べき剰余記号 $[p_1, p_2, p_3, p_4]$ の導入 s.t.

$$(-1)^{\mu_2(1234)} = [p_1, p_2, p_3, p_4].$$

5. 類体論と電磁双対性

平方剰余記号

$$\left(\frac{p}{q}\right) = \frac{\sigma_q(\sqrt{p})}{\sqrt{p}}$$

は「“関数” $\sqrt{p}$ が “Frobenius ループ” σ_q に沿って一回りしたときの変化=モノドロミー」とみることもできる．これは次のような物理的な状況を想起させる.

いま, Minkowski 時空 M の原点にモノポール (磁荷 b) があり, そのまわりを荷電粒子 (電荷 e) がループ C に沿い一回りするとする．モノポールが生むゲージ場 (磁場)=接続 1-形式を A とすると, 電荷の波動関数 ψ は次の微分方程式をみたす:

$$(d - A)\psi = 0.$$

従って, 電荷が C に沿って一回りしたときに波動関数 ψ が受ける影響 $\psi \mapsto (b, c)\psi$ はモノドロミー

$$(b, c) = \exp\left(\frac{ie}{\hbar}\oint_C A\right)$$

で与えられる.

ここで, 磁荷と電荷の役割を入れ替え, 今度は磁荷が電荷から受ける変化をモノドロミー (e, b) で表すと, “作用・反作用”の法則

$$(b, e) = (e, b)$$

が成り立つ. これは “平方剰余の相互律” に他ならない.

さて, C を境界とするお椀を考えて Stokes の定理を適用し, C を小さくしてお椀を (磁荷を囲む) 球面に近づけると, Dirac の量子化条件をえる:

$$eb = 2\pi i\hbar n \qquad (n \in \mathbb{Z}).$$

これより, $e \gg 1$(強結合領域) $\Leftrightarrow$ $b \ll 1$(弱結合領域) の関係にあり, これは次の類似を想起させる:

$e \gg 1 \quad \Longleftrightarrow \quad b \ll 1$ (強結合領域) $\overset{\text{双対}}{\longleftrightarrow}$ (弱結合領域) 難　　　　易	p : 大 $\quad \Longleftrightarrow \quad q$: 小 $x^2 \equiv q \bmod (p) \overset{\text{双対}}{\longleftrightarrow} x^2 \equiv p \bmod (q)$ 難　　　　易

最後に, 上で述べたまつわり数, 平方剰余と作用・反作用の三位一体の視点から, Poincaré 双対性, 類体論と電磁双対性を見直してみよう.

・<u>Poincaré 双対性</u>.

$$H^1(X_K) \simeq H_c^2(X_K)^* \qquad [\Sigma_K] \cup [L] = \mathrm{lk}(K, L).$$

・<u>類体論 (Artin-Verdier 双対性)</u>.

$$\begin{array}{ccccc} H^1(X_p) & \simeq & H_c^2(X_p)^* & & [\Sigma_p] \cup [q] = \left(\frac{p}{q}\right) \\ \shortparallel & & \shortparallel & & \\ \{\text{Galois 指標}\} & \simeq & \{\text{Hecke 指標}\} & & \text{可換 Langlands 対応} \end{array}$$

・<u>Maxwell 電磁双対性</u>.

$$H^2(M) \overset{\text{Hodge}*}{\simeq} H^2(M) \qquad \text{電場 } E \leftrightarrow \text{磁場 } B$$

さらに, 可換 Langlands 対応 ρ (Galois 指標) $\leftrightarrow$ $\mathcal{L}(\rho)$ (Hecke 指標) は L

関数の間の等式

$$\text{Artin}\, L \text{ 関数 } L(\rho, s) = L(\mathcal{L}(\rho), s) \text{ Hecke}\, L \text{ 関数}$$

をみたすが, これは次の量子論における電磁双対性 (可換 S-双対性) の類似とみることができる: A を電磁ポテンシャル, $F_A = E+B = dA, *F_A = dA'$ とする. このとき, 次の分配関数の間の等式が成り立つ: $eb = 1$ なら,

$$\begin{array}{ccc} Z(e) & = & Z(b) \\ \shortparallel & & \shortparallel \\ \int \mathcal{D}A \exp\left(-\frac{1}{e}\int_M F_A \wedge *F_A\right) & & \int \mathcal{D}A' \exp\left(-\frac{1}{b}\int_M F_{A'} \wedge *F_{A'}\right). \end{array}$$

まつわり数	平方剰余	作用・反作用
Poincaré 双対性	類体論	電磁双対性

Reference
M. Morishita, Knots and Primes – An Introduction to Arithmetic Topology, Universitext, Springer, 2011.