三次曲線の神秘

寺杣友秀

1. 振り子の周期と楕円積分

振り子の振動に関する微分方程式をたてて、その解を求めてみよう。点 O を中心に長さ 1 のひもで重さ 1 の質点 p がつながれている状況を考える。重力加速度は 1 として O を通り重力方向の直線のなす角度 θ を時間 t の関数として θ の満たす微分方程式を立ててみる。最大振れ幅を θ_0 とすると、最大に振れた時の位置エネルギーは一番下にある状態を起点とすると、$1-\cos(\theta_0)$ となる。角度が θ のときの位置エネルギーは $1-\cos(\theta)$ でそのときの速度は $\dfrac{d\theta}{dt}$ であることを考えれば、そこでの運動エネルギーは $\dfrac{1}{2}\big(\dfrac{d\theta}{dt}\big)^2$ となる。エネルギー保存則によると、位置エネルギーと運動エネルギーの和は常に一定で $1-\cos(\theta_0)$ となるので、

$$\frac{1}{2}\Big(\frac{d\theta}{dt}\Big)^2+1-\cos(\theta)=1-\cos(\theta_0)$$

となる。これは t に関する関数 $\theta=\theta(t)$ に関する微分方程式なので、これを解いてみよう。

$$\frac{1}{2}\Big(\frac{d\theta}{dt}\Big)^2=\cos\theta-\cos\theta_0,\quad \frac{d\theta}{dt}=\sqrt{2(\cos\theta-\cos\theta_0)}$$

となる。これは変数分離形の微分方程式なので、求積法で解くことができる。

$$dt=\frac{1}{\sqrt{2(\cos\theta-\cos\theta_0)}}d\theta$$

$$t=\int\frac{1}{\sqrt{2(\cos\theta-\cos\theta_0)}}d\theta+C$$

ただし C は積分定数である。三角関数が出てくる積分なので $u=\tan(\dfrac{\theta}{2})$ と変換すると、

$$\sin(\theta)=\frac{2u}{1+u^2},\quad \cos(\theta)=\frac{1-u^2}{1+u^2}$$

となり、

$$2(\cos\theta-\cos\theta_0)=\frac{4(u_0^2-u^2)}{(1+u^2)(1+u_0^2)}$$

$$d\theta=\frac{2du}{1+u^2}$$

なので、$u_0 = \tan(\frac{\theta_0}{2})$ とおくと、

$$\int \sqrt{\frac{(1+u^2)(1+u_0^2)}{4(u_0^2-u^2)}} \frac{2du}{1+u^2} = \sqrt{(1+u_0^2)} \int \frac{1}{\sqrt{(u_0^2-u^2)(1+u^2)}} du$$

なので、時間に関するスケール変換をして $-u_0$ から出発して u までかかる時間 t は

$$t = \int_{-u_0}^{u} \frac{1}{\sqrt{(u_0^2-u^2)(1+u^2)}} du$$

ということになる。逆に位置 u を時間に関する関数として求めるには $t = t(u)$ の逆関数 $u = u(t)$ を求めればよい。関数 $u(t)$ は積分の始点 u_0 の取り方に依存してきまるものである。$u = u(t)$ とあらわされる関数は楕円関数とわれ三角関数や対数関数、指数関数などの初等超越関数では表すことはできない。

2. 三角関数の加法定理の幾何学的証明

振り子の振動の方程式であるので $u = u(t)$ は時間 t に関して周期的な関数になることが予測される。これは実際にそうなって、その周期 p は

$$2\int_{-u_0}^{u_0} \frac{1}{\sqrt{(u_0^2-u^2)(1+u^2)}} du$$

となる。ここで 2 倍したのは、行きと帰りでは平方根の取り方において符号がが逆になるからである。

これは楕円関数の周期と言われる。つまり、この関数は $0 \leq t \leq P$ で定義されているが、これを $u(t) = u(t+P)$ という周期関数として定義したとき、これは無限回可微分関数関数となることが（証明はしないが）わかる。

周期的な関数の代表として三角関数があるが、三角関数と同じような性質が楕円関数にもあるのだろうか？例えば加法定理や倍角公式などは考えられるのだろうか？加法定理があればそこから倍角公式もでてくるはずである。そこで三角関数の類似を追ってみたいと思うのだが、そもそも三角関数は楕円関数のような積分としてあらわすとき、どのように定義されるのだろうか？

楕円関数は初めに逆関数から定義されていて、その逆関数は無理関数の積分として定義されていた。三角関数もそのようにして定義することができる。逆三角関数に関する微分の公式

$$\frac{d}{dx}(\sin^{-1}(x)) = \frac{1}{\sqrt{1-x^2}}$$

を用いて三角関数の加法公式を理解できないだろうか？この式から、$\sin(t) = x$ とおくと $x = x_0$ という点から $x = x_1$ で与えられる点まで運動するときにかかる時間は

$$t = \int_{x_0}^{x_1} \frac{dx}{\sqrt{1-x^2}}$$

で求められる。まず三角関数を点の運動としてとらえてみる。ここで時間は t とする。$x = x(t)$ として x の時間微分を求めてみると、$\frac{dx}{dt} = \sqrt{1-x^2}$ で与え

れらる。ここで位置と運動量 $y = y(t) = \dfrac{dx}{dt}$ を表す点 $(x(t), y(t))$ を各時間ごとにプロットすると曲線

$$x^2 + y^2 = 1$$

上を運動することがわかるだろう。

ご存知のように加法定理は次のような定理である。

$$\sin(\alpha + \beta) = \sin\alpha\cos\beta + \cos\alpha\sin\beta$$
$$\cos(\alpha + \beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta$$

この公式の素晴らしいところは、$\sin(\alpha+\beta), \cos(\alpha+\beta)$ が $\sin(\alpha), \sin(\beta), \cos(\alpha), \cos(\beta)$ を用いて代数的に書かれている点である。このような公式は楕円関数では望めないのか？

これを考えるために、三角関数の場合に加法定理が代数的に書かれているという事実を図形的に考えてみることは有用である。この運動において図形上の点 $p_0 = (1, 0)$ から $p_1 = (\cos\theta, \sin\theta)$ まで移動するのにかかる時間は θ である。$p_2 = (\cos\alpha, \sin\alpha)$ から初めて θ だけ時間がたったときの点を $p_3 = (\cos(\alpha+\theta), \sin(\alpha+\theta))$ とするときに p_3 の座標が p_0,p_1,p_2 の点の座標の多項式で書くことができればその形が加法定理となる。

点 p_3 を点 p_0, p_1, p_2 から図形的に求めるには以下のようにすればよい。まず p_1, p_2 を結ぶ直線 $L = \overline{p_1p_2}$ を考える。次に p_0 を通って L と平行な直線 L' を考えて L' の p_0 でない方の交点が p_3 になるのである。実はこのことは、射影平面 $\mathbf{P}^2$ で考えれば、これは次のように考えることができる。平面を射影平面に $(x, y) \mapsto (x : y : z)$ と埋め込むとその補集合は $(x : y : 0)$ であらわされる無限遠直線 L_∞ となる。p_1 と p_2 を結ぶ直線が無限遠直線 L_∞ と交わる点を p_{12} とおくと、p_{12} と p_0 を結んでできる直線と円 C の交点を考えたとき、その二つの交点のうちの p_0 ではない方が p_3 となるのである。実際上の図形的な方法で $p_3 = (\cos(\theta+\alpha), \sin(\theta+\alpha))$ を表せば、加法定理が得れらるのである。

3. 三次曲線と楕円積分

同様のことを楕円関数で考えてみよう。同様に点 $(u, w) = (u, \dfrac{du}{dt})$ を時間 t をパラメータとする運動と考えると

$$(\frac{du}{dt})^2 = (u_0^2 - u^2)(1 + u^2)$$

という微分方程式を満たすので、その軌跡を考えれば

$$w^2 = (u_0^2 - u^2)(1 + u^2)$$

という曲線上を動くことがわかる。この曲線は楕円曲線と呼ばれる。楕円曲線とは代数幾何的な概念で代数的な座標変換を施したものやはり楕円曲線よばれる。ここで

$$w = W(u_0 - U), u = U$$

という座標変換を考える。このとき (U, W) は

$$W^2(u_0 - U) = (u_0 + U)(1 + U^2)$$

で定義される曲線上を動くことがわかる。これは射影変換を施すことにより

$$y^2 = x^3 + ax + b$$

という形の方程式の平面３次曲線にすることができる。今度は三角関数のようにその軌跡が有理曲線になるわけではない。楕円曲線は代数的な変数変換で３次曲線として表すことができる。ここまでをまとめると、微分方程式を解くことにより、３次曲線の上を動く運動が得られる。

4. 三次曲線と加法

それでは楕円曲線の加法定理を 3 次曲線の幾何学を用いて求めることができるだろうか？円の場合は無限遠直線を補助にとることにより図形的に和の構造を定義してこれが時間に関する和の構造と一致することをみた。3 次曲線の場合もこれのまねをして加法の構造をいれることを考えよう。以後 3 次曲線

$$C^0 : y^2 = x^3 + ax + b$$

を複素射影平面 $\mathbf{P}^2 = \{(x : y : z) \mid (x, y, z) \neq (0, 0, 0)\}$ で考えるときは同次式

$$C : y^2 z = x^3 + axz^2 + z^3$$

によって定義されているものと思う。ここで C^0 から C に移行するときに新たに付け加わる点は $x = z = 0$ であらわされる点のみである。直線と 3 次曲線の交点を用いて 3 次曲線の上に加法を定義したい。加法を定義するときに一つ原点となるべき点 p_0 を固定して、ここだけの記号でこれを 0 と書く。p_1 と p_2 の和をつぎの様に定義する。

> p_1, p_2 を結ぶ直線と 3 次曲線 C の交点のうち p_1, p_2 でないもの
> を p_{12} とする。さらに p_{12} と 0 を結ぶ直線がと C の交点のうち
> $p_{12}, 0$ ではないものを $p_1 + p_2$ と定義する。

このとき交換法則 $p_1 + p_2 = p_2 + p_1$ および $0 + a = a$ は明らかに成り立つ。

定理 4.1. この加法は結合法則をみたす。つまり

$$(p_1 + p_2) + p_3 = p_1 + (p_2 + p_3)$$

を満たす。

補題 4.2. 次の点で縦横は一直線にあるとする。

$$\begin{array}{ccc} p_{12} & p_1 + p_2 & 0 \\ p_1 & x & p_2 + p_3 \\ p_2 & p_3 & p_{23} \end{array}$$

このとき x は C を通る。

Proof. 横の 3 本の直線を定義する方程式を考えてその積である 3 次の多項式 F_1 を考えると x 以外の 8 点で 0 となる。他方縦について同じことをするとやはり x 以外の 8 点で 0 になる 3 次多項式 f_2 が得られる。8 つの点で消える 3 次式全体の空間の次元は 2 次元なのでこれは F_1, F_2 で生成される 2 次元のベクトル空間になるので曲線 C も x を通る。 □

上の補題は結合法則を意味する。加法を計算するには、連立方程式

$$\begin{cases} y^2 = x^3 + ax + b \\ y = px + q \end{cases}$$

において二つの解がわかっているときにもう一つの解を求めるという操作を 2 回行えばよい。例えば $p_1 = (x_1, y_1), p_2 = (x_2, y_2)$ が上の連立方程式を満たすとして、もう一つの交点 p_{12} の座標を (x_3, y_3) とすると、x_3, y_3 は x_1, x_2, y_1, y_2 を用いて次のように表すことができる。まず x に関する 3 次方程式に変形して、

$$(px + q)^2 = x^3 + ax + b$$

なので、解と係数の関係から

$$x_1 + x_2 + x_3 = p^2$$

である。直線 $y = px + q$ の傾きは $p = \dfrac{y_1 - y_2}{x_1 - x_2}$ なので、

$$x_3 = \Big(\frac{y_1 - y_2}{x_1 - x_2}\Big)^2 - x_1 - x_2$$

となり、

$$y = \frac{y_1 - y_2}{x_1 - x_2}(x - x_1) + y_1$$

の x に x_3 を代入すれば、y_3 が求めらえる。

5. 加法と楕円関数

ここでは 3 次曲線の加法と楕円関数の加法の関係を示す。(u, w) を (x, y) に移す変換を施して方程式を

$$y^2 = x^3 + ax + b$$

と変換したとき、もとの変数 t と (u, w) の満たす微分方程式

$$dt = \frac{du}{w}$$

がどう変換されるかをまず見ておこう。前の章と違った変換を使うことにする。まず

$$w^2 = (u_0^2 - u^2)(1 + u^2) = (u_0 - u)(u_0 + u)(1 + u^2)$$

を次のようにして $y^2 = x^3 + ax + b$ の形に変換しよう。$u' = \dfrac{1}{u_0 - u}$ とおくと $u = \dfrac{1}{u'} + u_0$ なので u に関する 3 次式 $f(u)$ は $\dfrac{g(u')}{{u'}^3}$ の形に変換される。ここで $g(u')$ は u' に関する 3 次式である。したがって

$$w^2 = \frac{g(u')}{{u'}^4}, \quad (w^2 {u'}^2)^2 = g(u')$$

と変換される。したがって $y = w{u'}^2$ とすると

$$y^2 = g(u')$$

という形になるので、さらに $x = pu' + q$ なる一次変換を施すことにより、方程式は $y^2 = x^3 + ax + b$ の形に変換される。

このとき被積分関数は置換積分をもちいて

$$\frac{du}{w} = k\frac{dx}{y}$$

という形に変形される。ここで k は 0 ではい定数である。したがって変数 t を

$$t = t(x) = \int_{x_0}^{x} \frac{dx}{y} \ \Big(= \int_{x_0}^{x} \frac{dx}{\sqrt{x^3 + ax + b}} \Big)$$

と定義する。（定数倍の k により時間のスケールを変換をしたことになる。）

問題 5.1. 上の変換で被積分関数の変換を計算せよ。

次の定理が成り立つ。楕円関数を定義するときにの起点 (x_0, y_0) を起点とする積分により定義したものを $(x(t), y(t))$ とする。また (x_0, y_0) を原点として前の章のようにして 3 次曲線 C に加法を導入する。

定理 5.2. 3 次曲線の加法と楕円関数において時間の足し算で得られる加法は一致する。言い換えれば、楕円関数に関して加法定理

$$(x(t_1), y(t_1)) + (x(t_2), y(t_2)) = (x(t_1 + t_2), y(t_1 + t_2))$$

が成立する。

この定理を示すために直線と楕円曲線の交点の方程式

$$\begin{cases} y^2 = x^3 + ax + b \\ y = px + q \end{cases}$$

を考え、 3 つの交点を (x_1, y_1), (x_2, y_2), (x_3, y_3) とする。(p, q) が変化すると、直線 $L : y = px+q$ は変化するのでそれに応じて x_1 も変化するので、x_1 は (p, q) の関数とみることができる。ここで x_1, x_2, x_3 は 3 次方程式の解なので、解の番号付けの順番を一つ固定しなくてはならないので、ここでは (p, q) は微小変化を考えて、解の番号付けも連続になるようにとってくる。このとき $x_1 = x_1(p, q)$ という 2 変数関数で全微分可能なので、その全微分を

$$dx_1 = \frac{\partial x_1}{\partial p} dp + \frac{\partial x_1}{\partial q} dq$$

と書く。x_2, x_3, y_1, y_2, y_3 についても同様に考える。下の命題を証明する。

命題 5.3. t_1, t_2, t_3 を実数として、$x_i = x(t_i), y_i = y(t_i)$ とする。t_1, t_2, t_3 が三点 (x_1, y_1), (x_2, y_2), (x_3, y_3) 一直線上のっているという条件を満たすように動くとすると、$t_1 + t_2 + t_3$ は一定である。

命題をしめすためには p, q が微小変形されるとき、$t_1 + t_2 + t_3$ の微小変形が 0 であることを示せばよい。つまり、

$$dt_1 + dt_2 + dt_3 = \frac{dx_1}{y_1} + \frac{dx_2}{y_2} + \frac{dx_3}{y_3} = 0 \tag{5.1}$$

を示せばよい

$$\begin{aligned} &\frac{dx_1}{y_1} + \frac{dx_2}{y_2} + \frac{dx_3}{y_3} \\ =&\frac{dx_1}{px_1 + q} + \frac{dx_2}{px_1 + q} + \frac{dx_3}{px_1 + q} \\ =&\frac{(px_2 + q)(px_3 + q)dx_1 + (px_3 + q)(px_1 + q)dx_2 + (px_1 + q)(px_2 + q)dx_3}{(px_1 + q)(px_2 + q)(px_3 + q)} \end{aligned}$$

ここで分子を計算すると

$$\begin{aligned} &p^2(x_2x_3dx_1 + x_3x_1dx_2 + x_1x_2dx_3) \\ &+pq((x_1 + x_2)dx_3 + (x_2 + x_3)dx_1 + (x_3 + x_1)dx_2) \\ &+q^2(dx_1 + dx_2 + dx_3) \end{aligned} \tag{5.2}$$

ここで x_1, x_2, x_3 は 3 次方程式

$$(px+q)^2 = x^3 + ax + b$$

の解なので、

$$\begin{aligned} x_1 + x_2 + x_3 &= p^2 \\ x_1x_2 + x_2x_3 + x_3x_1 &= a - 2pq \\ x_1x_2x_3 &= q^2 - b \end{aligned}$$

が得られ、これらの式の全微分の式

$$\begin{aligned} dx_1 + dx_2 + dx_3 &= 2pdp \\ (x_1+x_2)dx_3 + (x_2+x_3)dx_1 + (x_3+x_1)dx_2 + &= -2pdq - 2qdp \\ x_1x_2dx_3 + x_2x_3dx_1 + x_3x_1dx_2 &= 2qdq \end{aligned}$$

を (5.2) に代入すると (5.1) が得られる。

6. 楕円曲線を複素数で考える

ここから楕円曲線 $C : y^2 = x^3 + ax + b$ を複素数で考える。射影平面上で C を考えるまえに平面 $\{(x,y) \mid x, y \in \mathbf{C}\}$ で考える。複素平面、あるいは複素数平面との混同をさけるためにこれはアファイン平面とよぶことにする。ここで集合

$$\{(x,y) \mid x, y \in \mathbf{C}, y^2 = x^3 + ax + b\}$$

はどのような形かを考えてみる。複素数の範囲で

$$x^3 + ax + b = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3), \quad (\alpha_1 + \alpha_2 + \alpha_3 = 0)$$

と因数分解できる。簡単のため、$\alpha_1, \alpha_2, \alpha_3$ が実数で $\alpha_1 < \alpha_2 < \alpha_3$ となる場合を考える。さて

$$y^2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$$

という曲線を考えたいのだが、y^2 が $x = \alpha_1, \alpha_2, \alpha_3$ でなければ、一つの x に対して二つの y が可能性としてありうるので、複素平面二つの貼り合わせで考えることにする。まずリーマン球面を二つ用意する。これらを α_1 と α_2 を結ぶ直線と α_3 と無限遠点を結ぶ直線で切れ目をいれて貼り合わせると、位相空間的にはトーラスと同相になる。

以上により C は複素平面 2 枚に切れ目をいれて貼り合わせたものとみることができる。C の中で $(x,y) = (\alpha_1, 0), (\alpha_2, 0), (\alpha_3, 0)$ の周りでは x を局所的な座標としてとると C 上の 2 点が同じ x に対応して不都合がおきる。そのまわりでは y を局所的な座標としてとると、C 上の点と y の値が 1 : 1 に対応する。座標は C 全体では定まらないが局所的には定まっている。しかも x と y はその両方が座標として考えられるところでは互いに他の正則関数として表されている。このような幾何学的対象はリーマン面とよばれる。正しい定義はさておき、次のことが言える。

> $C : y^2 = x^3 + ax + b$ を射影化した楕円曲線はリーマン面である。

7. 複素積分とリーマン面、２重周期

実数の範囲で考えたことを思いだすと、積分

$$t=\int_{\infty}^{x}\frac{dx}{\sqrt{(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)}}$$

であらわされた関数の逆写像 u は振り子の振動のところで述べたように周期

$$P=2\int_{\infty}^{\alpha_3}\frac{dx}{\sqrt{(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)}}$$

をもつ周期関数だったが、これは複素数の範囲で、つまりリーマン面で考えられないだろうか？つまり楕円積分を (1) 複素化すること、(2) 逆写像を考えること、という操作を行わないたい。目的を端的に言えば次のような $x=x(t)$ を定義したい。

(1) $x(t)$ という複素数 t に対して一意的に定義された複素数値関数 x が定義されて、
(2) x は P を周期とする周期関数である。つまり $x(t)=x(t+P)$ を満たす。

そのために積分

$$t=\int_{\infty}^{x}\frac{dx}{y}$$

を複素積分として定義する。$(\alpha_1,0)$ と (x,y) はともにリーマン面上の点とみなすと上の成分は $(\alpha_1,0)$ と (x,y) を結ぶ道の取り方による。正則関数の複素積分の性質からこれは道の連続変形によって値が変わらない。

このことを述べるために C の普遍被覆 $\widetilde{C}$ を定義しよう。このように $\widetilde{C}$ を定義すると、複素積分 t によって

$$\tau:\widetilde{C}\to\mathbf{C}$$

という写像が定まる。実際無限遠でもこの写像の値は確定して、コンパクト化した普遍被覆上の関数として定義される。実は下が成り立つ。

定理 7.1. 上の写像 τ は $1:1$ の全射である。リーマン面として”同型”である

さてここでは上の定理を認めることにする。このとき、γ_1,γ_2 を二つの閉じた道とするとき、τ_1,τ_2 を

$$\tau_1=\int_{\gamma_1}\frac{dx}{y},\quad \tau_2=\int_{\gamma_2}\frac{dx}{y}$$

と定義して、これを楕円関数の基本周期という。τ の逆関数 $(x,y)=(x(t),y(t))$ は二つの基本周期 τ_1,τ_2 をもつ周期関数である。つまり

$$x(t)=x(t+\tau_1),\quad x(t)=x(t+\tau_2)$$
$$y(t)=y(t+\tau_1),\quad y(t)=y(t+\tau_2)$$

となる。これから整数 a,b に対して

$$x(t)=x(t+a\tau_1+b\tau_2),\quad y(t)=y(t+a\tau_1+b\tau_2),$$

が成立することがわかる。このような性質をもつ関数を 2 重周期関数という。

$$L = L(\tau_1, \tau_2) = \{a\tau_1 + b\tau_2 \mid a, b \in \mathbf{Z}\}$$

は加法について閉じた集合となるが、これを周期格子という。一般に上の形の集合を格子と呼び、そのときに用いられる τ_1, τ_2 を格子の基底という。さらに τ_1 が τ_2 に対して半時計向きにあるとき (τ_1, τ_2) をむきつけれらた基底という。これは $\Im(\tau_1/\tau_2) > 0$ であることと同値である。

7.1. **周期格子の同値性.** 格子に現われる τ_1, τ_2 は $\mathbf{C}$ のベクトルとみたとき一次独立である。いま $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ を整係数で行列式が 1 となる行列とする。このような行列全体を $SL(2, \mathbf{Z})$ と書く。

問題 7.2. (1) $g_1, g_2 \in SL(2, \mathbf{Z})$ とすると $g_1 g_2 \in SL(2, \mathbf{Z})$ となる。
(2) $g \in SL(2, \mathbf{Z})$ とすると $g^{-1} \in SL(2, \mathbf{Z})$ となる。

問題 7.3. (1) τ_1, τ_2 が一次独立で、$g \in SL(2, \mathbf{Z})$ とすると

$$\begin{pmatrix} \tau_1' \\ \tau_2' \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \tau_1 \\ \tau_2 \end{pmatrix} \tag{7.1}$$

とすると、$L(\tau_1, \tau_2) = L(\tau_1', \tau_2')$ が成り立つ
(2) (τ_1, τ_2) と (τ_1', τ_2') を共に向き付けられた独立な元とする。$L(\tau_1, \tau_2) = L(\tau_1', \tau_2')$ が成り立つとき、ある $g \in SL(2, \mathbf{Z})$ が存在して *(7.1)* が成り立つ。これを証明せよ。

問題 7.4. α_1, α_2 を実数として、楕円曲線の方程式の形が $y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_1 - \alpha_2)$ となったとすると、独立な周期として一つは実数、一つは純虚数となるようにとることができる。

周期格子の同値性 L_1, L_2 を二つの格子とする。L_1 と L_2 が同値であるとはある $c \in \mathbf{C} - \{0\}$ が存在して

$$L_1 = cL_2 (= \{cu \mid u \in L\})$$

となることである。実は次の定理が成り立つ。

定理 7.5. 周期格子が同値であれば、楕円曲線

$$y^2 = x^3 + ax + b$$

は射影同値である。この対応によって格子の同値類の集合と 3 次曲線の射影同値類は *1* 対 *1* に対応する。

この定理の素晴らしいところは楕円関数の周期から楕円関数とその微分の軌跡の定める 3 次曲線が射影同値となってしまうところにある。3 次曲線は代数多様体と呼ばれるものに拡張される。このことは次の原理に一般化される。

原理 7.6. 積分周期は代数多様体の情報をたくさん含んでいる。

8. 楕円曲線のモジュライとモジュラー関数

8.1. **ラマヌジャンと分割関数について.** シュリニバーサ・ママヌジャン (1887-1920) インドのマドラスで事務官をしている傍ら、いくつもの神秘的な等式を発見する。現在では、それらの等式はほぼ証明されているが、当時は証明がつけられていないという理由でそれらの等式は正当な扱いをうけていなかった。

自然数 n を $a = \lambda_1 + \lambda_2 + \cdots + \lambda_p$ $(1 \leq p, 1 \leq \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_p)$ の形にあらわす仕方の個数は分割数と呼ばれ $p(n)$ と書かれる。

$$\frac{1}{\prod_{i=0}^{\infty}(1-q^i)} = 1 + p(1)q + p(2)q^2 +$$

という等式が得られる。

問題 8.1. 上の等式を証明せよ。

ラマヌジャンは分割数を非常によく近似する近似式を証明した。右辺の式を分割数の母関数という。

8.2. **ラマヌジャンの τ 関数.** デルタ関数は分割数の母関数と類似の式で

$$\Delta = (2\pi)^{12} q\{(1-q)(1-q^2)(1-q^3)\cdots\}^{24}$$

と定義される。$\dfrac{\Delta}{(2\pi)^{12}}$ を展開してえられた級数

$$q\{(1-q)(1-q^2)(1-q^3)\cdots\}^{24} = q + b_2q^2 + b_3q^3 + b_4q^4 + \cdots$$

を考えると整数の列 $b_1 = 1, b_2, b_3$ が得られる。上のテーラー展開の係数 b_n はラマヌジャン関数とよばれ $\tau(n)$ と書かれる。n が小さいところの値は下のようになる。

$$\tau(1) = 1, \tau(2) = -24, \tau(3) = 252, \tau(4) = -1472, \tau(5) = 4830, \tau(6) = -6048, \ldots$$

ラマヌジャンは次の性質を予想した。

(1) m, n を互いに素な自然数とするとき、$\tau(mn) = \tau(m)\tau(n)$.
(2) p を素数とするとき、

$$\tau(p^{n+2}) = \tau(p)\tau(p^{n+1}) - p^{11}\tau(p^n) \quad (n = 0, 1, 2, \ldots)$$

が成立する。
(3) $|\tau(p)| \leq 2p^{11/2}$

初めの二つはモーデルにより証明された。これは現代ではヘッケ作用素という群論的な構造との関連で証明される。三番目の予想は長い間懸案であったが、アイヒラーと志村の理論と久賀・志村多様体を用いることにより、ドリーニュがウェイユ予想に帰着することを証明した。さらに数年後ドリーニュ自身がヴェイユ予想を証明し、ラマヌジャン予想は完全に解決されたことになった。

9. 周期格子のモジュライと楕円曲線のモジュライ

9.1. **３次曲線曲線の射影同値類としての普遍量.** 変数変換

$$y = c^3y', x = c^2x'$$

によって方程式 $y^2 = x^3 + ax + b$ は

$$c^6y'^2 = c^6x'^3 + ac^2x' + b, \quad y'^2 = x'^3 + ac^{-4}x' + c^{-6}b,$$

より

$$a' = c^{-4}a, b' = c^{-6}b$$

とおくことにより再び同じ形の方程式 $y'^2 = x'^3 + a'x' + b'$ という同じ形の方程式が得られる。この変換において $a^3 : b^2 = a'^3 : b'^2$ は不変である。

問題 9.1. 射影変換で曲線 $y^2 = x^3 + ax + b$ が $y'^2 = x'^3 + a'x' + b'$ に移るとき、$a^2 : b^3 = a'^3 : b'^2$ が成り立つ。（9 つあるどの変曲点を無限遠にもっていっても同じ j の値が得られる。）

定義 9.2. 方程式を変形して

$$C : y^2 = 4x^3 - c_4x - c_6$$

とする。$j = j(C) = \dfrac{1728c_4^3}{c_4^3 - 27c_6^3}$ を楕円曲線の j 不変量という。

問題 9.3. ３次曲線が射影同値であるための必要十分条件は $j(C) = j(C')$ となることを示せ。

9.2. **周期格子の不変量.** 格子のむきつけられた基底 τ_1, τ_2 を考える。このとき $\tau = \tau_1/\tau_2$ とすると周期格子 $L(\tau_1, \tau_2)$ と $L(\tau, 1)$ は同値であることがわかる。このとき $\Im(\tau) > 0$ となる。集合

$$\mathbf{H} = \{\tau \in \mathbf{C} \mid \Im(\tau) > 0\}$$

を上半平面という。このとき τ を正規化周期という。

命題 9.4. $L(\tau, 1)$ と $L(\tau', 1)$ が同値であるとすると、ある $SL(2, \mathbf{Z})$ の元 $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ が存在して

$$\tau = \frac{a\tau' + b}{c\tau' + d} \tag{9.1}$$

が成り立つ。このとき $\tau = g(\tau')$ と書き、この式で与えられる座標変換を一次分数変換あるいはメビウス変換という。

Proof. 周期格子の同値性の定義より、ある $c \in \mathbf{C} - \{0\}$ が存在して、$L(\tau, 1) = kL(\tau', 1)$ となる。したがってある a, b, c, d が存在して

$$\tau = k(a\tau' + b), \quad 1 = k(c\tau' + d) \tag{9.2}$$

つまり、$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ と置くとき、

$$\begin{pmatrix} \tau \\ 1 \end{pmatrix} = kg \begin{pmatrix} \tau' \\ 1 \end{pmatrix}$$

が成り立つ。ここで $(\tau,1)$ と $(\tau',1)$ は同じ向きなので g は行列式が正となる整数係数行列である。また $L(\tau',1)=k^{-1}L(\tau',1)$ なので行列式が正である整数係数行列 $g'=\begin{pmatrix}a' & b'\\ c' & d'\end{pmatrix}$ が存在して、

$$\begin{pmatrix}\tau'\\1\end{pmatrix}=k^{-1}g'\begin{pmatrix}\tau\\1\end{pmatrix}$$

上の二つの式から

$$\begin{pmatrix}\tau\\1\end{pmatrix}=gg'\begin{pmatrix}\tau\\1\end{pmatrix}$$

という等式が得られるが $\tau,1$ は $\mathbf{R}$ 上一次独立なベクトルなので gg' は単位行列となる。したがって g は $SL(2,\mathbf{Z})$ の元である。式 (9.2) から $k=\dfrac{1}{c\tau'+d}$ なので

$$\tau=\frac{a\tau'+b}{c\tau'+d}$$

となる。 □

$\tau\in\mathbf{H}$ に対して次の無限級数を考える。

$$G_4=\sum_{p,q\in\mathbf{Z},(p,q)\neq(0,0)}\frac{1}{(p\tau+q)^4}$$
$$G_6=\sum_{p,q\in\mathbf{Z},(p,q)\neq(0,0)}\frac{1}{(p\tau+q)^6}$$

問題 9.5. 上の無限級数は収束することを証明せよ。

命題 9.6. $g=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ を $SL(2,\mathbf{Z})$ の元とする。τ に関する関数 $G_4(\tau)$, $G_6(\tau)$ を座標変換 *(9.1)* で τ' の関数に変換して得られた関数を $(G_4\mid_g)(\tau'),(G_6\mid_g)(\tau')$ と書く。このとき

$$(G_4\mid_g)(\tau')=(c\tau'+d)^4G_4(\tau') \tag{9.3}$$
$$(G_6\mid_g)(\tau')=(c\tau'+d)^6G_6(\tau')$$

したがって $L(\tau)$ と $L(\tau')$ が同値な周期格子であると

$$G_4^3(\tau):G_6^2(\tau)=G_4^3(\tau'):G_6^2(\tau')$$

が成立する。

問題 9.7. $G=G_4$ または G_6 とする。$(G\mid_g)(\tau')$ の τ' を τ で置き換えたものを $G\mid_g$ とかく。σ_1,σ_2 を $SL(2,\mathbf{Z})$ の元とするとき、

$$(G\mid_{\sigma_1})\mid_{\sigma_2}=G\mid_{\sigma_1\sigma_2}$$

を確かめよ

10. 楕円曲線の j 不変量

格子の不変量として G_4^3/G_6^2(解析幾何学的不変量) という量が得られた。一方 3 次曲線の不変量として a^3/b^2（代数幾何学的不変量）が得られた。実はこれらには次の関係がある

定理 10.1. $g_4 = 40G_4, g_6 = 140G_5$ とおくと、

(1) $\Delta = g_4^3 - 27g_6^3$ が成り立つ。Δ はラマヌジャンのところで出てきたものである。
(2) 格子の同値類に対して下の式で 3 次方程式の j 不変量は計算される。

$$j(C) = \frac{1728g_4^3}{g_4^3 - 27g_6^3}$$

11. 有限体上の楕円曲線と志村—谷山予想

1994 年フェルマーの最終定理がついにワイルスによって証明された。証明の手法は志村—谷山予想の少し条件がついたもとで解決することによって証明されたのだ。志村—谷山予想を述べるためにはアイヒラー—志村対応を述べることが必要で、この対応はラマヌジャン予想の解決へのステップにもなった。現代の数論において最も基本的かつ重要な対応である。これはラングランズ予想として予想が一般化されている。ラングランズ予想が解決されるのは、まだまだ遠い未来のことであろう。

アイヒラー志村対応の一つの鍵である、有限体上の楕円曲線の合同ゼータ関数については初等的に述べることができるので、ここで少し紹介することにしよう。ただし事実は「述べる」ことはできても、その背後に隠された「意味」については説明することは、決して難しいものではないのだが、（むしろとても単純なものであるが）新しいものの見方をする訓練が必要であるので、ここではできない。

代数で大切な概念に「体」という数の概念がある。大まかにいって和と交換可能な積が定義されていて、さらに 0 でないものに関して商が定義されているものである。n を 2 以上の自然数とする。例えば、整数を n を法として和と積が定義できることはご存知と思うが、一般に 0 でないものが必ずしも逆元をもつとは限らない。したがって一般にはそのような数体系は「体」ではないが n が素数 p のときに限り、0 ではいものは逆元をもつ。したがってそのようなとき整数を p を法として整数を考えると「体」になり、多くの代数幾何はほぼ平行に展開できる。このような数体系を有限体といい $\mathbf{F}_p$ と書く。

例えば $\mathbf{P}^1$ を $\mathbf{F}_p$ でも考えたることができ、それを $\mathbf{P}^1(\mathbf{F}_p)$ と書く。このとき比を考えればその個数は $p+1$ となる。同様に $\mathbf{P}^2$ の個数は p^2+p+1 となる。これは $(p^3-1)/(p-1)$ と計算しても、あるいは無限遠直線 $\mathbf{P}^1(\mathbf{F}_p)$ とアファイン平面の和集合として数えてもどちらでも一致する。

$$E : y^2 = x^3 - x$$

を（前の様に斉次化して）$\mathbf{P}^2(\mathbf{F}_p)$ の部分集合としても考えることができる。これを $E(\mathbf{F}_p)$ と書くことにする。

問題 11.1. $E(\mathbf{F}_p)$ の個数 $\#E(\mathbf{F}_p)$ には何かの規則性があるだろうか？

p	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$\#E(\mathbf{F}_p)$	4	8	8	12	8	16	20	24	40	32	40	32	44	48
$\#E(\mathbf{F}_p)-1-p$	0	2	0	0	-6	-2	0	0	10	0	2	-10	0	0

$\#E(\mathbf{F}_p)$ は表の様になっている。

この $\alpha_p = 1+p-\#E(\mathbf{F}_p)$ は保型形式という関数の係数（の一部分）となっているというのが志村谷山予想の典型的な例となっている。保型形式とは関数等式 (9.3) を満たす関数のことである。保型形式は純粋に関数論的に特徴付けられる関数なのであるが、このような関数の空間は有限次元であり、代数的性格をもつ関数群となっている。こういったものの代数性の基礎つけをあたえたのが、ヘッケやアイヒラーであり、志村五郎であった。

α_p はある線形写像のトレースとなっている。この線形写像を定義するのは二通りの仕方があって、ひとつはヘッケ作用素という関数論的に導かれるもので、もう一つはフロベニウス作用素という、有限体特有の幾何から生まれるものである。複素多様体の性質から導かれるものと、有限体の性質から導かれるものの一致という、不思議な対応はヴェイユ予想とあいまって、数学の世界に大変大きな衝撃を与えた。ドゥリーニュの師匠にあたるグロタンディークはこの二つを結びつけることを念頭に環論を基礎にエタール・コホモロジーの理論を切り開いたのである。グロタンディークはこういった一連の数論の問題に対して抽象代数の理論が不可欠であることを初めて提唱した数学者といえる。そういった意味でグロタンディークは２０世紀最大の数学者の一人であることは歴史の判断を待つまでもないだろう。

参考文献

下の二つは名著の誉高く、おすすめしたい本であるが、絶版になっていて、古本は高価なのが残念。英語版は手にはいるし、明快な英文なので気持ちよく読めると思う。

「数論講義」7 章、セール、岩波書店 (Serre, A Course in Arithmetic)
「複素解析」7 章、アールフォース、現代数学社 (Ahalfors, Complex Analysis)