応用楕円曲線論　プリント No.1

情報科学科　金子　晃

はしがき

この講義では有限体上の楕円曲線の概要とその暗号理論への応用を解説します．予備知識は学部の代数の標準的な講義の内容だけです．ただし, 古典的な背景も知っておいた方が後の理解を助けるでしょうから, 初回は関数論っぽいお話をします.

第 1 章　楕円曲線の古典的背景

この章では標数 0 の (普通の) 楕円曲線とそれに関連する数学のお話を概観します.

§1.1 楕円積分と楕円函数

1 8 世紀から，次の形の積分が応用数学でしばしば必要とされました.

$$\int \frac{1}{\sqrt{f(x)}}dx \tag{1.1}$$

ここに $f(x)$ は x の 3 次または 4 次の多項式です．$f(x)$ が 2 次式なら，逆三角函数 $\mathrm{Arcsin}\, x$ や $\mathrm{Arccos}\, x$ でこの積分は表現できますが，3 次以上の式だと，平方因子を持つとかの幸運な例外を除き，厳密な値は求まりません.

この形の積分は，振り子の運動を振れ角が小さいときの近似 $\sin x \doteqdot x$ を用いずに厳密に解こうとすると現れるのが代表例ですが，純粋数学でも，例えば，2 次曲線の弧長を計算しようとすると，放物線や円などの特別な場合以外は必ずこの形の積分になってしまい，正確な値が求まりません．特に楕円の弧長を表すことから，楕円積分という名前が付きました.

この積分が初等函数では表せないことが厳密に証明されたのは 1 9 世紀中ごろの Liouville によりますが，楕円の弧長の計算が難しいことは既に 17 世紀中ごろには認識されていたようで，この積分が新しい函数を与えるであろうことは多くの数学者が予感していたのです．積分

$$\int \frac{1}{\sqrt{1-x^2}} \tag{1.2}$$

自身ではなく，その逆函数が $\sin x$ という周期函数，すなわち単位円周 S^1 上の一価な函数を与えることから類推して，

$$\int \frac{1}{\sqrt{1-x^4}} \tag{1.3}$$

の逆函数を考えることに思い到ったのが，ガウス，そしてアーベルとヤコビです[1)]．こうして，楕円函数が発見されました．この函数は複素変数にすると，2 重周期を持つことが分かりました．$\sin x$ は複素変数にしても周期は一つの方向だけで，円柱 $\boldsymbol{R} \times iS^1$ 上の一価函数と思えます．2 重周期を持つような函数は，実軸方向にも丸くなっているので, トーラス $T^2 = S^1 \times S^1$ のような曲面の上で一価に定義されているものとみなせます.

[1)] Gauss は 1800 年前後, レムニスケートの弧長を調べるため, 上の積分を研究し, 逆函数が二重周期性を持つことを発見. 楕円函数の殆どの結果を得ましたが，例によって理論が熟するまで発表せず, すべては遺稿として残されました. その間に Abel が 1820 年代に,

$$\int_0^x \frac{1}{\sqrt{(1-c^2x^2)(1+e^2x^2)}}dx$$

の型の積分の逆函数として二重周期函数が得られることを発見，これを一般化した Abel 積分の理論を構築しました．更に Jacobi は 1820 ∼ 30 年代, ϑ 函数, $\mathrm{sn}(x)$ (sinusoidal), $\mathrm{cn}(x)$ (cnoidal) 函数に当たる楕円函数の変種を導入し, Abel の後を受けて楕円函数論の基礎付けをしたのです.

$S^1 = \boldsymbol{R}/\boldsymbol{Z}$ と思えるので，$T^2 = \boldsymbol{R}^2/\boldsymbol{Z}^2$ と考えられます．ここで，割り算はアーベル群の部分群による商の意味で，一般論により再びアーベル群になります．$\boldsymbol{R}^2 = \boldsymbol{C}$ とみなせるので，2 重周期を持つ複素解析函数は，例えば

$$\varphi_k(z) = \sum_{m,n=-\infty}^{\infty} \frac{1}{(z-m-in)^k} \tag{1.4}$$

のようなものを考えれば容易に作ることができます．これは $z=0$ に k 位の極を持つ解析函数となるのですが，この級数は m, n が大きいところでほぼ

$$(-1)^k \sum_{m,n=-\infty}^{\infty} \frac{1}{(m+in)^k}$$

に等しく，

$$\Big|\frac{1}{m+in}\Big| = \frac{1}{\sqrt{m^2+n^2}}$$

なので，残念ながら $k \geq 3$ でないと収束しません．しかし，$k=2$ でも，次のように工夫すると収束します：原点で発散する定数部分を引き去ると，

$$\varphi_2(z) = \frac{1}{z^2} + \sum_{(m,n)\neq(0,0)} \Big(\frac{1}{(z-m-in)^2} - \frac{1}{(m+in)^2}\Big) \tag{1.5}$$

1 位の極しか持たないような函数も，ちょっと工夫すれば作ることができます：

$$\psi(z) = \frac{1}{z} - \frac{1}{z-\alpha} + \sum_{(m,n)\neq(0,0)} \Big\{\Big(\frac{1}{z-m-in} + \frac{1}{m+in}\Big) - \Big(\frac{1}{z-\alpha-m-in} + \frac{1}{\alpha+m+in}\Big)\Big\} \tag{1.6}$$

ここに，α は $0 \leq \mathrm{Re}\,\alpha < 1$, $0 \leq \mathrm{Im}\,\alpha < 1$, $\alpha \neq 0$ を満たす任意の複素数です．こちらは $z=0$ と $z=\alpha$ にそれぞれ 1 位の極を持ち，それぞれにおける留数の和は 0 となっています．

一位の極を一つだけしか持たないような 2 重周期函数はどう頑張っても作ることができません．なぜでしょう？ これは実は Riemann 面上で一般に成り立つ Riemann-Roch の定理から出て来る結論です．

問題 1.1 上の和 (1.4) ～ (1.6) が z について広義一様に収束すること，より具体的には, 任意の $M > 0$ に対し，$|z| \leq M$ なら，N を十分大きく取るとき，M, N のみに依存する定数 C が存在して $\sqrt{m^2+n^2} \geq N$ に対し，一般項が

$$\leq \frac{C}{\sqrt{m^2+n^2}^3}$$

となることを示せ.

§1.2 楕円曲線

楕円曲線は，楕円とは全く異なり,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.7}$$

の形の方程式で定義される 3 次曲線です．今考えている実数や複素数のように，係数体の標数 $\neq 2$ のときは，簡単な線型座標変換で

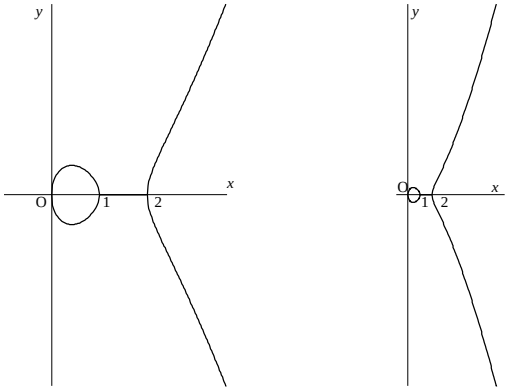
$$y^2 = x^3 + ax^2 + bx + c \tag{1.8}$$

の形にまで持って来られます．更に, 標数 $\neq 3$ でもあれば, x の 1 次または 2 次の項を消すこともでき，例えば

$$y^2 = 4x^3 - g_2x - g_3 \tag{1.9}$$

の形にできます[2)]．これらは Weierstrass の標準形と呼ばれます.

例 $y^2 = x(x-1)(x-a)$ $(a>1)$ と因数分解される場合．下図は $a=2$ のときで, 左が拡大図です.



$x \to \infty$ のとき分枝は $y \sim x^{3/2}$ で増大し, 無限遠点 $(0, \pm 1, 0)$ に向かいます.

§1.3 楕円曲線の群構造

楕円曲線 E 上の点の全体は以下に示すような幾何学的に定義された演算で可換群を成します．Bachet は既に 1621 年に, $y^2 = x^3 + c$ に対し 2 倍公式を発見し, この不定方程式の一つの有理解から他の有理解を作るのに利用していました, 一般の加法公式が発見されたのはもっと後で，群として認識されたのは 1 9 世紀になってからです．そもそも群の概念は 1 9 世紀前半の Galois に始まるものです.

加法の定義 曲線 $y^2 = x^3 + ax^2 + bx + c$ 上の点 $\mathrm{P} \in E$ と $\mathrm{Q} \in E$ を通る直線が再び曲線 E と交わる点を R' とするとき, R' を x 軸に関して線対称に写した点 R を $\mathrm{R} = \mathrm{P} + \mathrm{Q}$ と定める.

具体的には, $\mathrm{P} = (x_1, y_1)$, $\mathrm{Q} = (x_2, y_2)$, $\mathrm{R} = \mathrm{P} + \mathrm{Q} = (x_3, y_3)$ と置くとき,

$$x_3 = \lambda^2 - a - x_1 - x_2, \quad y_3 = -\lambda x_3 - \nu, \tag{1.10}$$

ここに

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \qquad \nu = y_1 - \lambda x_1 = y_2 - \lambda x_2 \tag{1.11}$$

これを加法公式と呼ぶ．$\mathrm{P} = \mathrm{Q}$ のときは, P, Q を通る直線を接線と解釈して $\mathrm{R} = 2\mathrm{P}$ が

$$x_3 = \lambda^2 - a - 2x_1, \quad y_3 = -\lambda x_3 - \nu, \tag{1.12}$$

ここに

$$\lambda = \frac{3x_1^2 + 2ax_1 + b}{2y_1}, \qquad \nu = y_1 - \lambda x_1 \tag{1.13}$$

で定義される．これを 2 倍公式と呼ぶ.

公式の証明 $\mathrm{P}(x_1, y_1)$, $\mathrm{Q}(x_2, y_2)$ を通る直線の方程式は

$$y = \lambda x + \nu, \quad \text{ここに} \quad \lambda = \frac{y_2 - y_1}{x_2 - x_1},\ \nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$$

よって $\mathrm{R}' = (x_3, -y_3)$ とすれば, x は

$$x^3 + ax^2 + bx + c - (\lambda x + \nu)^2 = (x - x_1)(x - x_2)(x - x_3) = 0$$

の第 3 の根 x_3 である．根と係数の関係より $x_1 + x_2 + x_3 = -a + \lambda^2$．よって $x_3 = \lambda^2 - a - x_1 - x_2$

[2)] 体の標数 p とは, $p \cdot 1 = 0$ となる最小の正整数のことで, 次回からキーワードとなりますが, 本日のところは $\boldsymbol{R}$ や $\boldsymbol{C}$ など, 標数 0 の普通の体だけ考えておけば十分です.

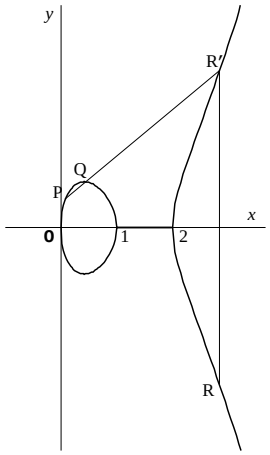
P = Q のとき, 一般に曲線 $f(x,y)=0$ 上の点 (x_1,y_1) における接線の方程式は

$$\frac{\partial f}{\partial x}(x_1,y_1)(x-x_1)+\frac{\partial f}{\partial y}(x_1,y_1)(y-y_1)=0$$

(接線とは一次近似なり！でしたね) 代数ではこれを接線の定義式とします. f は多項式なので重根条件からも導けます. 今は $f(x,y)=x^3+ax^2+bx+c-y^2$ なので, P を通る E の接線は

$$(3x_1^2+2ax_1+b)(x-x_1)-2y_1(y-y_1)=0$$

つまり $\lambda=\dfrac{3x_1^2+2ax_1+b}{2y_1}$, $\nu=y_1-\lambda x_1$. よってこれが E と再び交わる点 $(x_3,-y_3)$ は上と同様で, $x_3=\lambda^2-a-2x_1$.



別解 P = Q のときの公式から極限に行けば得られます：

$$y_1^2=x_1^3+ax_1^2+bx_1+c,\quad y_2^2=x_2^3+ax_2^2+bx_2+c$$

より,

$$\begin{aligned}\frac{y_2-y_1}{x_2-x_1}&=\frac{y_2^2-y_1^2}{(y_2+y_1)(x_2-x_1)}=\frac{(x_2^3+ax_2^2+bx_2+c)-(x_2^3+ax_2^2+bx_2+c)}{(y_2+y_1)(x_2-x_1)}\\&=\frac{1}{y_2+y_1}\Big(\frac{x_2^3-x_1^3}{x_2-x_1}+a\frac{x_2^2-x_1^2}{x_2-x_1}+b\Big)\end{aligned}$$

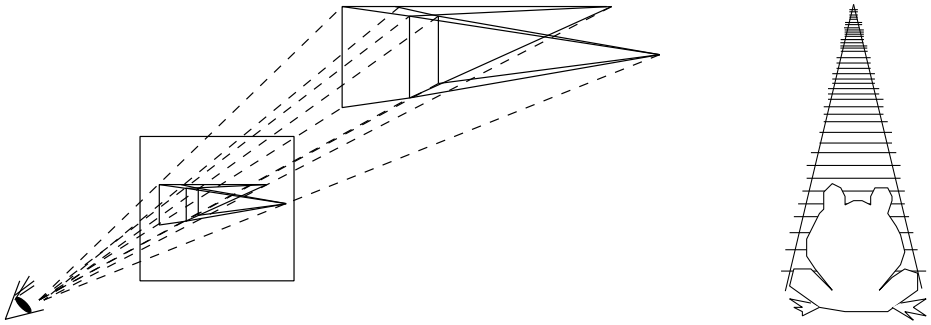
から $x_2\to x_1$ とすれば, $\dfrac{y_2-y_1}{x_2-x_1}\to\dfrac{3x_1^2+2ax_1+b}{2y_1}$.

Q 一般の方程式 (1.7) において $a_1\neq 0$ の場合には, P の逆元 $-P$ は x 軸に関する折り返しよりは複雑になります. 加法公式の形も少し違ってきます. 標数が 2 の場合はそのような曲線も考える必要があるので, 後に議論されます.

§1.4 無限遠点と射影幾何

群であることを言うには，単位元を定義しなければなりません．単位元は楕円曲線の唯一の無限遠点 $\mathcal{O}=(0,1,0)$ がそれです. 直感的には，この点は，楕円曲線の上の点が遠ざかって行ったときの極限位置 (といっても収束するわけではなく，方向が次第に $(0,1)$ の方に向かって行くというだけのことです．これを代数的に厳密に導くには, 射影平面の説明が必要になります．今まで用いて来た $\boldsymbol{R^2}$ はアフィン平面と呼ばれるものですが，これに無限遠の点を追加したものが射影平面です.

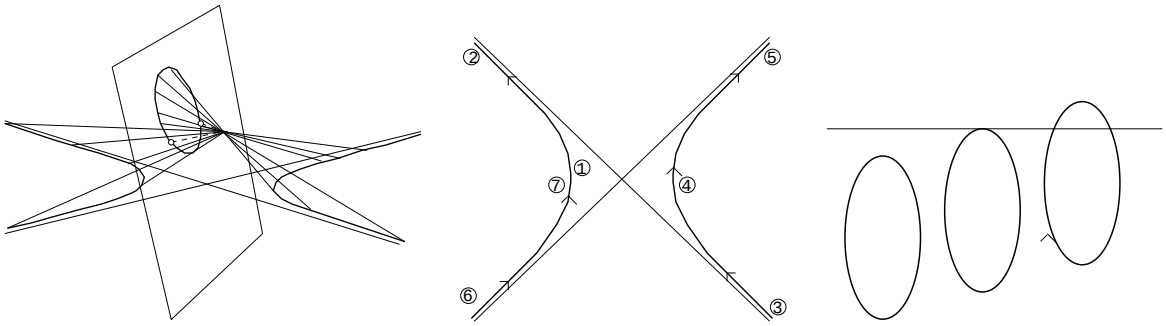
射影幾何はルネサンス時代に生まれた透視図法の数学的正当化として数学に導入されました. 透視図法とは，風景を立体的に見えるように平面に描く技術で, 現代の CG でも基本技法として用いられています．これを簡単に体現するには，景色を眼で見える通りにキャンパスにプロットしてゆけばよい. これは, 射影変換の典型例である配景変換 (perspective transform) となります：



実際の景色における無限遠点たちが，キャンパス上では，普通の直線上に並んでいますね．このように，射影幾何では射影変換により，無限遠にある直線は普通の有限直線と全く平等に扱われます．射影幾何における無限遠点の取り扱いで特徴的なのは，方向の±を区別しないことです．ある方向にどんどん進むと，無限遠点に到り，反対側 (背中) から戻って来ます．つまり，射影平面上では，どんな直線も，円周のように閉じているのです．また, 射影幾何には平行線というものはありません．アフィン平行 2 直線は無限遠の 1 点で交わります.

このような概念を解析的に表現するため，同次座標というものを用いて射影平面の点を三つの座標 $(X,Y,Z) \neq (0,0,0)$ で表します．ただし，比 $X:Y:Z$ が同じものは，同じ点を表すものとします．従って, $Z \neq 0$ なら，これですべてを割り算して，$=(x,y,1)$, $x = X/Z$, $y = Y/Z$ と書き直せます．これがアフィン平面の普通の座標に相当します．$Z = 0$ はそれ以外の点で，これが無限遠直線の方程式となります．同次座標で書くと，普通の直線も無限遠直線も，みな $aX + bY + cZ = 0$ という 1 次同次式の形に表されます．このときの係数の組 (a,b,c) は，$\neq (0,0,0)$ なら何でも良く，かつ明らかにそれらの比だけが問題なので，点の同次座標と全く区別がありません．このゆえに平面射影幾何では，点と直線との間にきれいな双対関係が成り立つのです.

代数曲線論はアフィン平面 $\boldsymbol{R}^2$ ではなく射影平面 $(\boldsymbol{R}^3 \setminus \{(0,0,0)\})/\boldsymbol{R}^\times$ で考えるのが普通です．これにより，2 次曲線は，楕円に統一されます．双曲線は，無限遠直線と交わる楕円，放物線は無限遠直線に接する楕円です.



楕円曲線を射影平面の同次座標 (X,Y,Z) を用いて書き直すには，$x = X/Z$, $y = Y/Z$ をもとの方程式に代入し，分母を払えばよい：

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3 \tag{1.14}$$

この上に有る無限遠点を求めるには，$Z = 0$ と置けばよく, $X^3 = 0$, つまり $X = 0$, よって解は $(0,Y,0)$ のみです. $Y \neq 0$ で割れば，これは $(0,1,0)$ となります.

§1.5 群の公理

上に導入した無限遠点 $\mathcal{O}$ が単位元となることは，幾何学的直感ではあきらかですね．正確に証明するには，加法公式を同次座標対応に書き直せばよいのですが，めんどうなのでやめておきましょう.

P の逆元は，−P，すなわち，y 座標の符号を反転したものです.

$\mathrm{P} + (-\mathrm{P}) = \mathcal{O} \iff$ P を通り, y 軸に平行な直線が $\mathcal{O}$ を通ります.

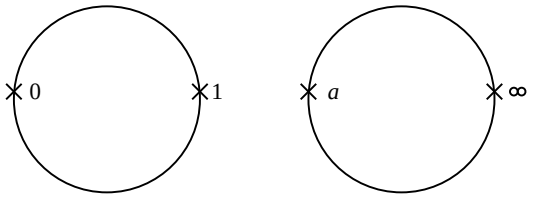
以上の演算の定義で E が群となることの証明は次の通りです：

◎単位元 $\mathcal{O}$ の存在, 逆元 $-\mathrm{P}$ の存在, は明らか
◎演算が可換なことも明らか.
◎結合律 $(\mathrm{P}+\mathrm{Q})+\mathrm{R}=\mathrm{P}+(\mathrm{Q}+\mathrm{R})$ の証明は全然自明でない.
直接計算してもできる. 幾何学的にも示せる. いずれもかなりやっかいです.

問題 1.2 上の演算に対し, 結合律を証明せよ. 計算にはフリーの数式処理ソフト Risa/Asir を使え (情報セキュリティ演習の課題!).

§1.6 複素数で見た楕円曲線

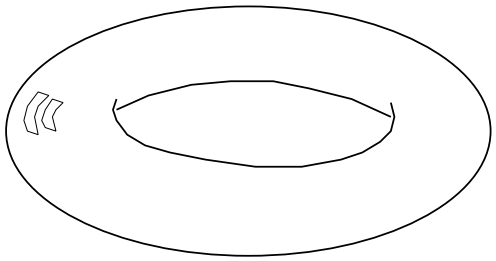
最初に述べた楕円積分と楕円曲線の関係がまだ見えて来ませんが, これを示すには, 実数の上だけで議論していたのではだめです. 無限遠点 $(0,\pm 1,0)$ は実は一つの点なので, 楕円曲線はここで繋がっています. この点を有限の位置に持って来ると, 次のような形となります：



Q 厳密にいうと, 線型の射影変換ではこの形にはできません. 双方向に有理式で表現できるような, いわゆる双有理変換が必要となりますが, その結果, 4 次の曲線 $y^2=(x^2-1)(4-x^2)$ などで上の形が実現できます.

問題 1.3 $y^2=x(x-1)(x-a)$ を $y^2=(x^2-1)(x^2-4)$ に写すような双有理変換を探せ.

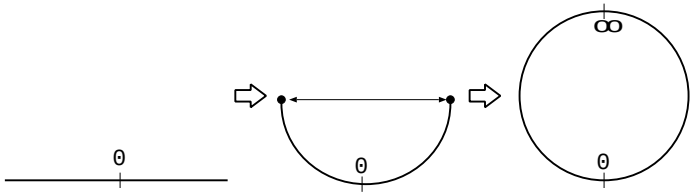
これだけじゃあ何だか分からないが, x, y を複素数で動かすと, 上は次のような曲面 (トーラス) の断面であることが分かります. これが代数幾何で普通に楕円曲線と呼ばれているものです：



§1.7 Riemann 面

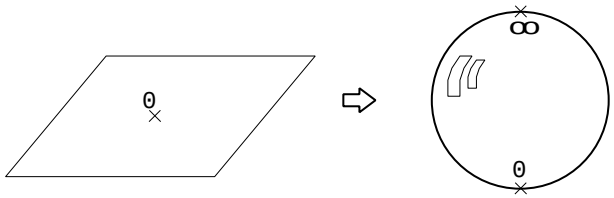
上では射影平面, すなわち, 実 2 次元の射影空間を考察しましたが, 射影空間は何次元でも同様に考えることができます. 実 1 次元のアフィン空間は直線ですが, 無限遠点を追加すると実射影直線になります. これは円周と同じ (位相) 構造をしています：

$$\boldsymbol{P}^1 := (\boldsymbol{R}^2 \setminus \{(0,0)\})/\boldsymbol{R}^\times$$

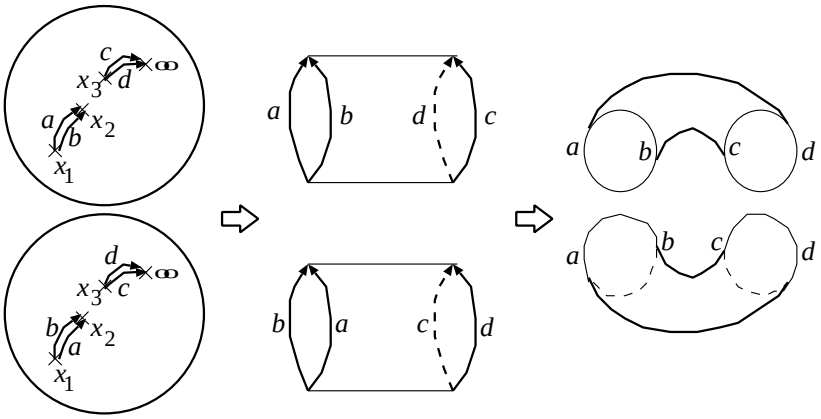


これに対し，複素 1 次元の空間は，いわゆる複素平面です．(２０年程前に高名な代数幾何学者が，教科書審議会で，複素平面は実は複素直線だとつぶやいたのが元で，高校の教科書の“複素平面”という用語が“複素数平面”になってしまったのは有名な話です．(^^;) これに無限遠点を追加すると複素射影直線になります．直線といっても，これは平面の 1 点コンパクト化ですから，球面と同じ構造を持つ，いわゆる Riemann 球面です：

$$\boldsymbol{CP}^1 = (\boldsymbol{C}^2 \setminus \{(0,0)\})/\boldsymbol{C}^\times$$

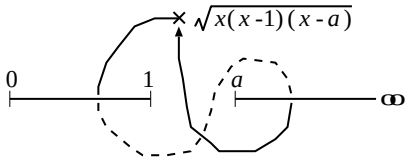


複素楕円曲線 $y^2 = x^3 + ax^2 + bx + c$ は x を Riemann 球面で動かし, $y = \pm\sqrt{x^3 + ax^2 + bx + c} = \pm\sqrt{(x - x_1)(x - x_2)(x - x_3)}$ のグラフとして実現できます．$x^3 + ax^2 + bx + c = 0$ の三根 x_1, x_2, x_3, および無限遠点では y の値が一つしかありません．そこで, Riemann 球面を二枚用意し, これらの点で切り開いて貼り合わせると，次のような図形ができます：

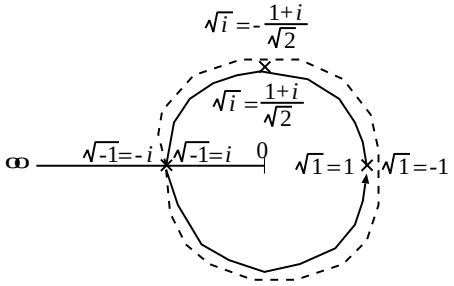


抽象的な多様体論が完成する前は，すべての Riemann 面は，このように Riemann 球面の分岐被覆として理解されていました．Riemann は函数論の基礎を築いた人ですが，1850 年代, Riemann 面の概念を導入し, Abel 多様体論の萌芽を与えました．Riemann 面を抽象多様体論の立場から初めて厳密に記述したのが２０世紀初の H. Weyl の著書 『Riemann 面』です．

上の曲面は, $y^2 = x^3 + ax^2 + bx + c$ の“高さを無視した”グラフです．これは多価函数 $\sqrt{z^3 + az^2 + bz + c}$ がその上で一価函数となるように定義域を修正したものとも思えます．これが函数 $\sqrt{z^3 + az^2 + bz + c}$ の Riemann 面です．

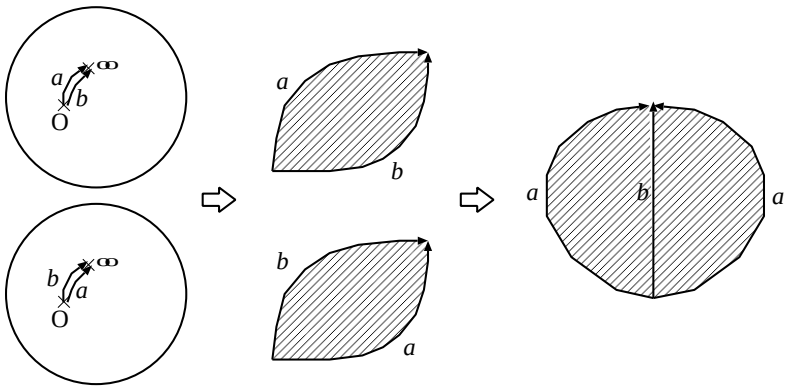


練習として, $y^2 = x$ の場合, i.e. $\sqrt{z}$ の Riemann 面をやってみましょう：



$y=\sqrt{x}$ は複素平面で $x=0$ を一周すると別の分枝になる.

複素平面を正の実軸に沿って無限遠点まで鋏を入れたものを二枚用意し, 一方の紙の切り口の上側と他方の紙の下側を貼り付けると, 分枝のこの変化が表現できます. これが $\sqrt{z}$ の Riemann 面です :



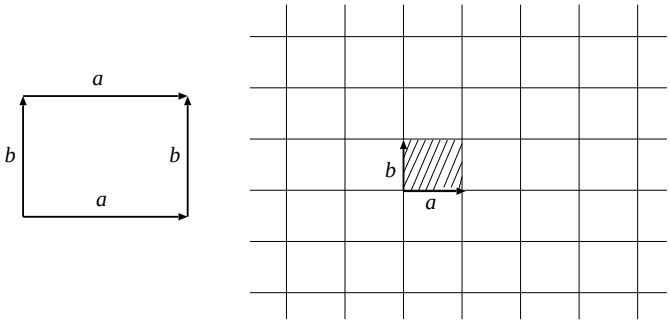
この場合は貼り合わせの結果は, 元の Riemann 球面と同じものに戻ってしまいます. これは函数 $\sqrt{z}$ が本質的に新しい函数をもたらさないことを意味しています.

§1.8 格子から作る楕円曲線

トーラスを作るには, 次のようにするのが最も簡単です :

> 四角い紙を用意し, 左右の辺を同一視すると輪になる.
> 更に上下の辺を同一視するとトーラスができる.

これは, 平面上の点 (x,y) と点 $(x+a,y)$ を, および, 点 (x,y) と点 $(x,y+b)$ を同一視するのと同等です :



直感的にはトーラスを作るために紙を丸めなければならないので, しわがよったりする心配をするかもしれませんが, 抽象数学としては, 単に同一視するだけなので, 無理に紙をひねって貼り合わせる必要はありません. 平面上を移動していって格子に達したら一瞬でワープし, 一つ手前の格子に戻ってしまうような世界を想像すればよいのです.

数学ではトーラスを $\boldsymbol{R}^2/L$ で定義します．ここに $L = \{(am, bn) \mid m, n \in \boldsymbol{Z}\}$ は $\boldsymbol{R}^2$ の離散部分加群で, 標準格子 (standard lattice) と呼ばれるものです.

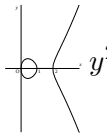
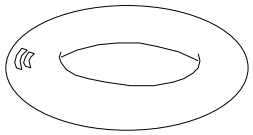
これを一般化し，ベクトル $a\boldsymbol{e}_1$, $b\boldsymbol{e}_2$ の代わりに $\boldsymbol{R}$ 上 1 次独立な (複素) 平面の任意のベクトル対 $\boldsymbol{a}, \boldsymbol{b}$ を取ってもよい：

$$\text{一般の格子：}\ L = \boldsymbol{Z}\boldsymbol{a} + \boldsymbol{Z}\boldsymbol{b} \quad \boldsymbol{a},\boldsymbol{b}\text{で張られる}\boldsymbol{R}^2\text{の部分加群}$$

$\boldsymbol{R}^2$ を複素平面 $\boldsymbol{C}$ だと思うと, ω_1, ω_2 を $\boldsymbol{R}$ 上 1 次独立な二つの複素数として,

$$T = \boldsymbol{C}/L, \quad L = \boldsymbol{Z}\omega_1 + \boldsymbol{Z}\omega_2$$

以上の構造からは, トーラスが加群となっていることが明らかです．すなわち，T の演算 $+$ は単に $\boldsymbol{R}^2$, あるいは $\boldsymbol{C}$ の演算 $+$ から商群に自然に誘導されたものとなります．では，


$y^2 = x^3 + ax^2 + bx + c$ と

$\boldsymbol{C}/L$ はほんとに同じ？

もしそうなら，楕円曲線の群構造は明らかですが，まだ両者の関係は形が似ているぞという程度におぼろげにしか見えていません.

§1.9 楕円函数；トーラスと楕円曲線の対応

トーラス T と楕円曲線 E の同等性は, 古典的な楕円函数で両者が対応することから分かるのです. この手法は，抽象的に定義された多様体を Euclid 空間に埋め込んで具体的に捉えるときなどによく用いられるものです．まず,

$\boldsymbol{C}/(\boldsymbol{Z}\omega_1 + \boldsymbol{Z}\omega_2)$ の上に函数 $f(z)$ が存在
$\iff$ $\boldsymbol{C}$ 上の函数 $f(z)$ で, 二重周期性：
$\quad f(z + m\omega_1 + n\omega_2) = f(z) \quad \forall\, m, n \in \boldsymbol{Z}$ を持つものが存在

に注意しましょう．このようなものの作り方は既に注意しました．最も基本的な函数は Weierstrass のペー函数と呼ばれる，次のものです.

$$\wp(z) := \frac{1}{z^2} + \sum_{(m,n)\in\boldsymbol{Z}^2\setminus(0,0)} \Big\{ \frac{1}{(z - m\omega_1 - n\omega_2)^2} - \frac{1}{(m\omega_1 + n\omega_2)^2} \Big\}$$

(Weierstrass は 1840 ∼ 60 年代, 冪級数を主体として函数論の厳密化を行い，楕円函数の解析的理論を構築しました．彼の手書きの p である $\wp$ は, その後も使い続けられ, 今では AMS-TeX の記号 `\wp` にも採り入れられています.) ここで,

$$\begin{aligned}
&\Big\{ \frac{1}{(z - m\omega_1 - n\omega_2)^2} - \frac{1}{(m\omega_1 + n\omega_2)^2} \Big\} \\
&= \Big\{ \frac{1}{(m\omega_1 + n\omega_2)^2} \frac{1}{\{1 - z/(m\omega_1 + n\omega_2)\}^2} - \frac{1}{(m\omega_1 + n\omega_2)^2} \Big\} \\
&= \Big\{ \frac{1}{(m\omega_1 + n\omega_2)^2} \Big(\frac{m\omega_1 + n\omega_2}{1 - z/(m\omega_1 + n\omega_2)} \Big)' - \frac{1}{(m\omega_1 + n\omega_2)^2} \Big\} \\
&= \Big\{ \frac{1}{(m\omega_1 + n\omega_2)^2} \sum_{k=0}^{\infty} \frac{(k+1)z^k}{(m\omega_1 + n\omega_2)^k} - \frac{1}{(m\omega_1 + n\omega_2)^2} \Big\} \\
&= \sum_{k=1}^{\infty} \frac{(k+1)z^k}{(m\omega_1 + n\omega_2)^{k+2}}
\end{aligned}$$

ここで更に奇数次の項の m,n に関する和は対称性により消えるので

$$\therefore\ \wp(z)=\frac{1}{z^2}+\sum_{(m,n)\in\boldsymbol{Z}^2\setminus(0,0)}\sum_{k=1}^{\infty}\frac{(2k+1)z^{2k}}{(m\omega_1+n\omega_2)^{2k+2}}=\frac{1}{z^2}+\sum_{k=1}^{\infty}(2k+1)G_{k+1}z^{2k}$$

$$\text{ここに } G_k:=\sum_{(m,n)\in\boldsymbol{Z}^2\setminus(0,0)}\frac{1}{(m\omega_1+n\omega_2)^{2k}},\quad k=2,3,\dots$$

すると,

$$\wp'(z)=-2\sum_{m,n=-\infty}^{\infty}\frac{1}{(z-m\omega_1-n\omega_2)^3}$$

$$\wp'(z+m\omega_1+n\omega_2)=\wp'(z),$$

$$\wp(-z)=\wp(z),\quad \wp'(-z)=-\wp'(z),$$

$$\wp'(\frac{\omega_1}{2})=\wp'(\frac{\omega_2}{2})=\wp'(\frac{\omega_1+\omega_2}{2})=0,$$

$$\wp'(z)^2=4\wp(z)^3-g_2\wp(z)-g_3,\quad \text{ここに}\ \ g_2=60G_2,\ g_3=140G_3$$

が得られます. 最後の等式の証明は簡単なのでやっておきましょう. $z=0$ で極が消えていることを言えば, 差は全平面で有界正則となるので, Liouville の定理より定数となります. 従って更に, $z=0$ で定数項も消えていることを言えば, 差は恒等的に 0 となり, 証明が完了します.

$$\wp(z)=\frac{1}{z^2}+3G_2z^2+5G_3z^4+\cdots$$

を項別微分して,

$$\wp'(z)=-\frac{2}{z^3}+6G_2z+20G_4z^3+\cdots$$

$$\therefore\ \wp'(z)^2-4\wp(z)^3=\Big(\frac{4}{z^6}-\frac{24G_2}{z^2}-80G_4+\cdots\Big)-4\Big(\frac{1}{z^6}+\frac{9G_2}{z^2}+15G_3+\cdots\Big)=-\frac{60G_2}{z^2}-140G_3$$

よって, g_2, g_3 を上のように選べば, 確かに極と定数項が消えます. これより,

$$\begin{array}{ccc}\boldsymbol{C}/(\boldsymbol{Z}\omega_1+\boldsymbol{Z}\omega_2) & \xrightarrow{\sim} & E:=\{(x,y)\in\boldsymbol{CP}^2\mid y^2=4x^3-g_2x-g_3\}\\ \cup & & \cup\\ z & \mapsto & (\wp(z),\wp'(z))\end{array}$$

という対応が定まります. これが同型対応となっていることをきちんと調べるのは演習問題としておきましょう.

さて，楕円函数には，加法公式と呼ばれる重要な公式があります．このような公式は，楕円函数が発見される前に，既に Euler により 18 世紀に，楕円積分の間の種々の関係式の一つとして実質的には知られていたものです.

$$\wp(u+v)=-\wp(u)-\wp(v)+\frac{1}{4}\Big(\frac{\wp'(u)-\wp'(v)}{\wp(u)-\wp(v)}\Big)^2 \tag{1.15}$$

上の対応により，$\boldsymbol{C}$ の加法が $\wp(z)$ の加法定理を通して楕円曲線の演算に対応しているのです．このことをきちんと調べるのも演習問題としておきましょう.

問題 1.4 $\wp$ 函数の加法公式 (1.15) を証明してみよ.［ヒント：微分方程式を使え.］

問題 1.5 $\boldsymbol{C}$ の加法が $\wp(z)$ の加法定理を通して幾何学的に定義された楕円曲線の演算に対応していることを確かめよ.

問題 1.6 下記のような特別な場合の方程式について, 実でのグラフ, 複素形 (Riemann 面), 加群の構造がそれぞれどうなるか調べよ.

1) $y^2=x(x-1)^2$ (右辺が 2 重根を持つ).
2) $y^2=x^3$ (右辺が 3 重根を持つ).
3) $y^2=x(x^2+1)$ (右辺が 1 実根のみを持つ).