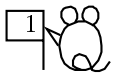
幾何入門　第２回

情報科学科　金子　晃
Алексей　КАНЕНКО
kanenko@is.ocha.ac.jp
この講義のホームページ:
http://atom.is.ocha.ac.jp/~kanenko/KOUGI/Geo
この講義のホームディレクトリ:
edusv.edu.is.ocha.ac.jp/~kanenko/Geo

射影変換



同次座標を線型に変換する：

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \mapsto \begin{pmatrix} \xi \\ \eta \\ \zeta \end{pmatrix} = \begin{pmatrix} a & b & e \\ c & d & f \\ g & h & k \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

結果は同次座標として確定すればよいので,
行列全体を $\boldsymbol{R}^\times$ の元で割っても変換としては同じもの.

よって

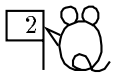
射影変換群　$PGL(2,\boldsymbol{R}) = GL(3,\boldsymbol{R})/\boldsymbol{R}^\times$

直線 $gx+hy+kz=0$ が変換後の無限遠直線 $\zeta=0$ に対応する.

無限遠直線 $z=0$ は直線 $\xi = ax+by, \eta = cx+dy, \zeta = gx+hy$ に対応する.

これから x, y を消去して $\begin{vmatrix} \xi & a & b \\ \eta & c & d \\ \zeta & g & h \end{vmatrix} = 0$

アフィン変換と射影変換



無限遠直線を動かさない射影変換はアフィン変換となる：
$z = 0 \Longrightarrow \zeta = gx + hy = 0$ となるためには, $g = h = 0$.
従って $k \neq 0$ なので, これで行列全体を割算すると

$$\begin{pmatrix} \xi \\ \eta \\ 1 \end{pmatrix} = \begin{pmatrix} a & b & e \\ c & d & f \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} \quad \text{の形}$$

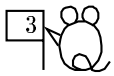
書き直すと

$$\begin{cases} \xi = ax + by + e, \\ \eta = cx + dy + f \end{cases} \quad \text{あるいは} \quad \begin{pmatrix} \xi \\ \eta \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} e \\ f \end{pmatrix}$$

CG の世界では最初の形をアフィン変換の同次座標表示と呼んでいる.

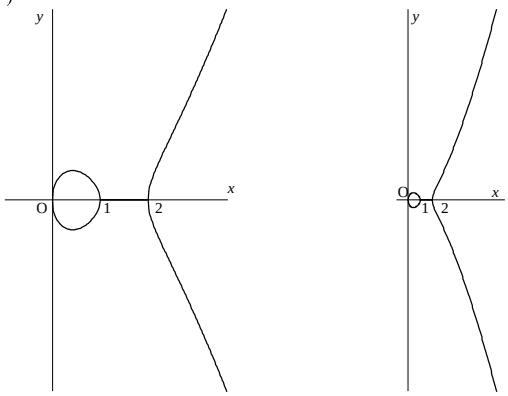
問題 **3** y 軸を y 軸に写し, 無限遠直線を直線 $x = 1$ に写すような
射影変換の行列の形を決定せよ.
この変換で直線族 $x = n$, $n = 1, 2, \ldots$ はどんな図形に写るか？

楕円曲線



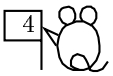
この頃暗号の世界で流行っているもの.
楕円とは全く異なり, $y^2 = x^3 + ax^2 + bx + c$ の形の方程式で定義される.

例 $y^2 = x(x-1)(x-a)$ $(a > 1)$ と因数分解される場合
(図は $a = 2$)



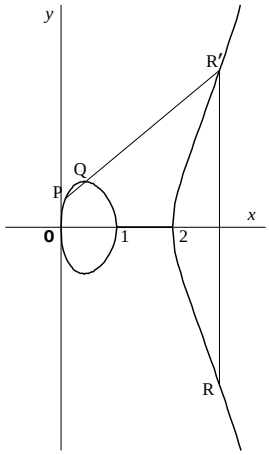
$x \to \infty$ のとき分枝は $y \sim x^{3/2}$ で増大し, 無限遠点 $(0, \pm 1, 0)$ に向かう.

楕円曲線の群構造



楕円曲線 E 上の点の全体は可換群を成す：
曲線上の点 $\mathrm{P} \in E$ 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,

$$x_3 = \lambda^2 - a - x_1 - x_2, \quad y_3 = -\lambda x_3 - \nu,$$
$$\text{ここに} \quad \lambda = \frac{y_2 - y_1}{x_2 - x_1},$$
$$\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$$

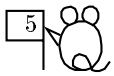


$\mathrm{P} = \mathrm{Q}$ のときは, P, Q を通る直線を接線と解釈して $\mathrm{R} = 2\mathrm{P}$ は

$$x_3 = \lambda^2 - a - 2x_1, \quad y_3 = -\lambda x_3 - \nu,$$
$$\text{ここに} \quad \lambda = \frac{3x_1^2 + 2ax_1 + b}{2y_1},$$
$$\nu = y_1 - \lambda x_1$$

無限遠点 $\mathcal{O} = (0, 1, 0)$ は単位元となる.

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



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

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

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

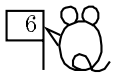
の第3の根 x_3 である.
根と係数の関係より $x_1 + x_2 + x_3 = -a + \lambda^2$

$$\therefore \quad x_3 = \lambda^2 - a - x_1 - x_2$$

$\mathrm{P} = \mathrm{Q}$ 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！)
代数ではこれを定義式とする. f は多項式なので重根条件から導ける.



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る：

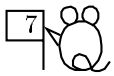
$$y_1^2=x_1^3+ax_1^2+bx_1+c,\quad y_2^2=x_2^3+ax_2^2+bx_2+c$$

より,

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

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

群の公理



楕円曲線 E の無限遠点はただ一点 $\mathcal{O}=(0,1,0)$.

これを代数的に厳密に導くには, 同次座標を用いて

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$$

としておいて $Z=0$ と置けば, $X^3=0$, つまり $X=0$,
よって解は $(0,Y,0)$ のみ. $Y\neq 0$ で割れば $(0,1,0)$ となる.

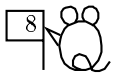
$\mathrm{P}+(-\mathrm{P})=\mathcal{O} \iff \mathrm{P}$ を通り, y 軸に平行な直線が $\mathcal{O}$ を通る.

以上の演算の定義で E が群となることの証明 :

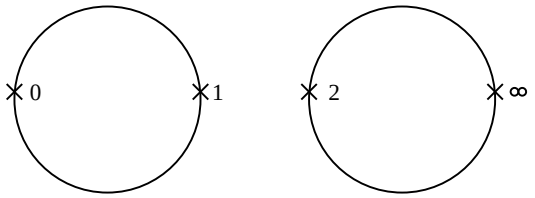
◎単位元 $\mathcal{O}$ の存在, 逆元 $-\mathrm{P}$ の存在, は明らか
◎演算が可換なことも明らか.
◎結合律 $(\mathrm{P}+\mathrm{Q})+\mathrm{R}=\mathrm{P}+(\mathrm{Q}+\mathrm{R})$ の証明は自明でない.
　直接計算してもできる. 幾何学的にも示せる.

問題 **4**　上の演算に対し, 結合律を証明せよ.

複素数で見た楕円曲線

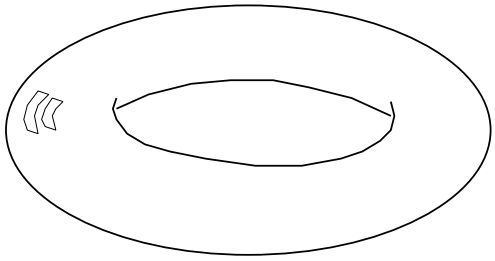


無限遠点 $(0, \pm 1, 0)$ は実は一つの点なので, 曲線はここで繋がっている.
この点を有限の位置に持って来ると, 次のような形となる：

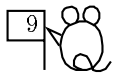



厳密にいうと,
線型の射影変換では
この形にはできない.
4 次の曲線
$y^2 = (x^2 - 1)(4 - x^2)$
などで実現できる.

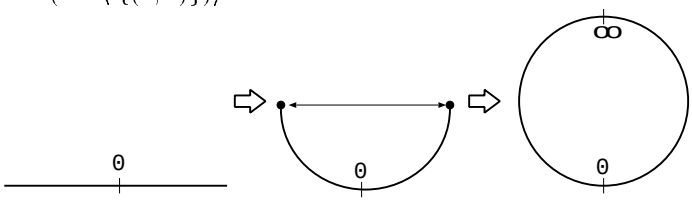
これだけじゃあ何だか分からないが, x, y を複素数で動かすと,
上は次のような曲面の断面であることが分かる：



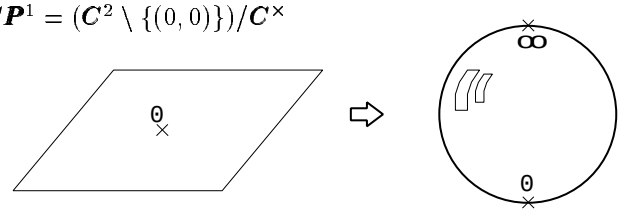
実数と複素数



実一次元のアフィン空間は直線
無限遠点を追加すると実射影直線になる $\Longleftrightarrow$ 円周と同じ構造
$\boldsymbol{P}^1 := (\boldsymbol{R}^2 \setminus \{(0,0)\})/\boldsymbol{R}^\times$

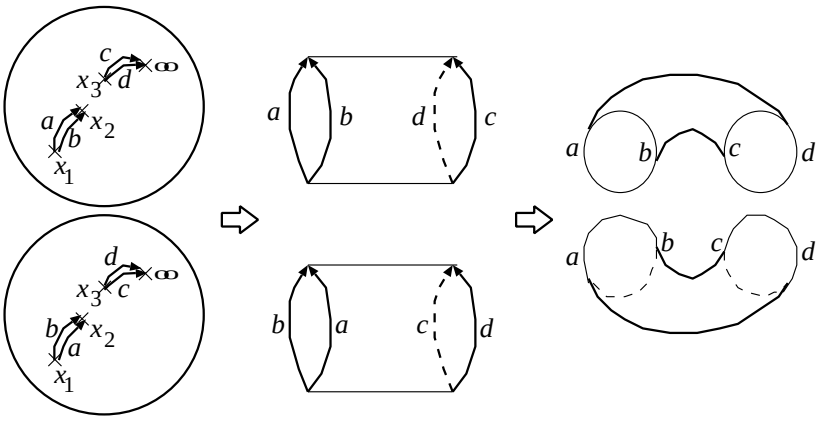


複素一次元の空間は平面 (いわゆる複素平面)
無限遠点を追加すると複素射影直線になる
$\Longleftrightarrow$ 球面と同じ構造 (Riemann 球面)
$\boldsymbol{CP}^1 = (\boldsymbol{C}^2 \setminus \{(0,0)\})/\boldsymbol{C}^\times$



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る.
$x^3 + ax^2 + bx + c = 0$ の三根 x_1, x_2, x_3, および無限遠点では
y の値が一つしかない.

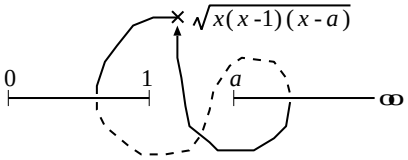
そこで, Riemann 球面を二枚用意し, これらの点で切り開いて貼り合わせる：



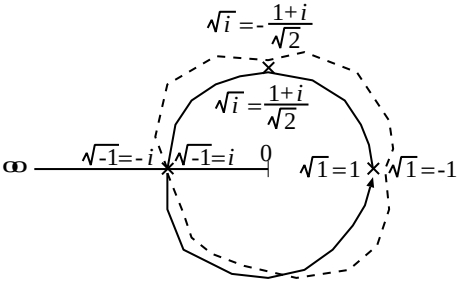
Riemann 球面の分岐被覆としての Riemann 面

上の曲面は, $y^2 = x^3 + ax^2 + bx + c$ の “ 高さを無視した ” グラフ.
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る.

$\Longrightarrow$ $\sqrt{z^3 + az^2 + bz + c}$ の
Riemann 面

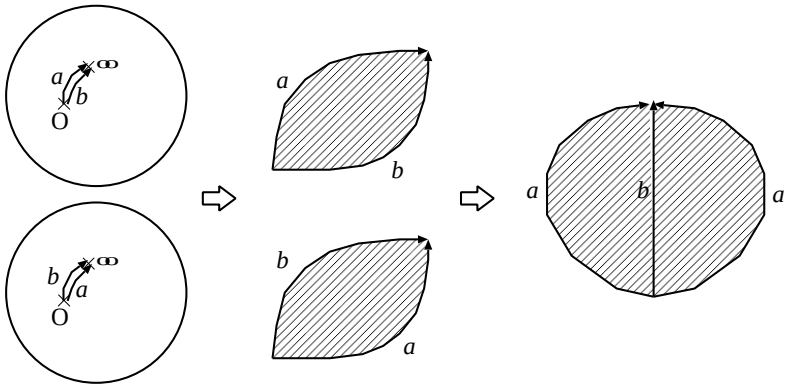


練習として, $y^2 = x$ の場合, i.e. $\sqrt{z}$ の Riemann 面をやっておく：



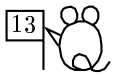
$y = \sqrt{x}$ は複素平面で
$x = 0$ を一周すると
別の分枝になる.

$\Longrightarrow$ 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,
分枝の変化が表現できる ($\sqrt{z}$ の Riemann 面) :

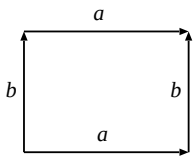


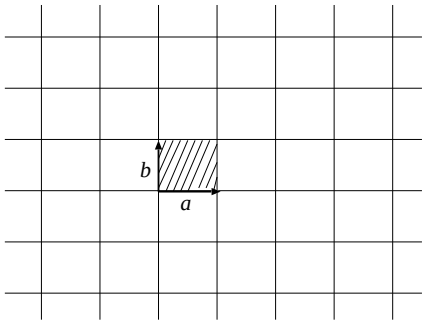
この場合は貼り合わせの結果は, 元の Riemann 球面と同じものに戻る.

最も簡単なトーラスの作り方



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, 平面で (x, y) と $(x + a, y)$ および, (x, y) と $(x, y + b)$ を
同一視するのと同等:





単に同一視するので, 無理に紙をひねって貼り合わせる必要はない.
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.

数学ではトーラスを $\boldsymbol{R}^2/L$ で定義する.
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.

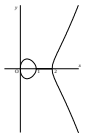
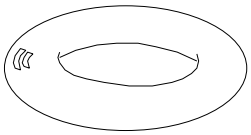
ベクトル ae_1, be_2 は一次独立な一般のベクトル $\boldsymbol{a}$, $\boldsymbol{b}$ で取り替えてもよい：

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

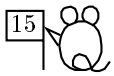
$\boldsymbol{R}^2$ を複素平面 $\boldsymbol{C}$ だと思うと, ω_1, ω_2 を $\boldsymbol{R}$ 上一次独立な二つの複素数として,

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

この構造からは, トーラスが加群となっていることが明らか：
　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.


$y^2 = x^3 + ax^2 + bx + c$ と

$\boldsymbol{C}/L$ は
ほんとに同じもの？

楕円函数



トーラス T と楕円曲線 E の同等性は, 楕円函数というもので
両者が対応することから分かる.

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

このようなものを作れと言われたら, 例えば

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

なんていうのをすぐ考え付くだろう.
ただし, これでは収束しない (2 次元的和なので, 収束には冪 > 2 が必要).
普通は $z = 0$ での Laurent 展開の定数項が 0 となるように定数を調節した

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

が用いられる (Weierstrass の $\wp$ 函数).

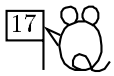
さて

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

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

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

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



すると,

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

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

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

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

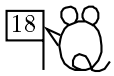
$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3, \quad \text{ここに} \ \ g_2 = 60G_2,\ g_3 = 140G_3$$

(最後の等式の証明は, $z=0$ で極だけ消えていることを見れば十分.
$\Longleftarrow$ Liouville の定理)

これより,

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

という対応が定まる.
$\boldsymbol{C}$ 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.



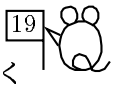
問題 5 下記のような特別な場合の方程式について,
実でのグラフ, 複素形 (Riemann 面), 加群の構造が
それぞれどうなるか調べよ.
勇気の有る人は, 格子による商群としての表現も調べて見よ.

1) $y^2 = x(x-1)^2$ (右辺が二重根を持つ).

2) $y^2 = x^3$ (右辺が三重根を持つ).

3) $y^2 = x(x^2+1)$ (右辺が一実根のみを持つ).

楕円曲線と楕円函数の歴史



(このページを正確にしようと思っているうちにずいぶん遅く
なってしまったので, とりあえず暫定版であきらめます.)

二重周期性を持つ楕円函数は, 楕円の弧長を求めるとき出て来る積分
$\int_0^x \frac{1}{\sqrt{1-x^4}}dx$ の逆函数として発見された

c.f. 円の弧長に関連する積分 $\int_0^x \frac{1}{\sqrt{1-x^2}}dx$ の逆函数として
周期性を持つ函数 (i.e. 円周上の一価函数) $\sin x$, $\cos x$ が得られる.

楕円曲線という名前は, それが楕円函数の自然な定義域なので付けられたもの. 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.

☆ Bachet 1621, $y^2 = x^3 + c$ 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

☆ Euler 18 世紀, 楕円積分の間の種々の関係式 (加法定理など) を導く

☆ Gauss 1800 年前後, レムニスケートの弧長を調べるため, 積分
$\int_0^x \frac{1}{\sqrt{1-x^4}}dx$ 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たが発表せず, 遺稿として残された.

☆ Abel 1820 年代, $\int_0^x \frac{1}{\sqrt{(1-c^2x^2)(1+e^2x^2)}}dx$ 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

☆ Jacobi 1820 ∼ 30 年代, ϑ 函数, $\mathrm{sn}(x)$ (sinusoidal), $\mathrm{cn}(x)$ (cnoidal) 函数に当たるものを導入し, Abel の後を受けて楕円函数論の基礎付けをした

☆ Riemann 1850 年代, Riemann 面の概念を導入し, Abel 多様体論の萌芽を与えた

☆ Weierstrass 1840 ∼ 60 年代, $\wp$ 函数を導入し, 解析的理論を構築