黒木玄 **Gen Kuroki**
@genkuroki

楕円曲線にはWeierstrass form以外にも実用的に使われている表示がたくさんあります。

Jacobi form

$$z^2 = (1-y^2)(1-k^2y^2).$$

Edwards form

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

これらはJacobiの楕円函数でパラメトライズされます。Edwards formでの加法公式はシンプルになり、その場合は楕円曲線暗号として実際に使われています(実際には捻られた場合なのですが)。Jacobiの楕円函数がシンプルな加法公式を生み出すことは実際に「実用的」だったわけです。詳しくは "Ed25519" について検索してみて下さい。

Hessian form

$$x^3+y^3+1 = axy$$

はこれの射影化

$$x^3+y^3+z^3 = axyz$$

が有名だと思う。

他の様々な表示については
hyperelliptic.org/EFD/

2017年05月06日 13:37 · Web · 0 · ★ 2 · Webで開く

黒木玄 **Gen Kuroki** @genkuroki on May 6
Ed25519を使っている意識の高い人達は本質的にJacobiの楕円函数の加法公式がシンプルであることによって得られる「効率性」と「安全性」を利用していることになります。

黒木玄 **Gen Kuroki** @genkuroki on May 6
私は学生時代にJacobiの楕円函数について勉強したときに、面倒な計算でうんざりし、その後、テータ函数で計算した方が色々楽になることに気付き、Jacobiの楕円函数を自分で使うことはほぼ無くなりました。

しかし、最近、Edwards曲線

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

の件について知り、Jacobiの楕円函数を嫌う必要はないと思うようになれました。

Edwards曲線の式は $k=0$ で円になります。だからEdwards曲線は円を楕円曲線に一般化する一つの方法になっています。

円には自然にアーベル群構造が入ります。楕円曲線にもアーベル群構造が入る。(楕円曲線のアーベル群構造が楕円曲線暗号で使われている。) Edwards曲線を使えば円と楕円曲線のアーベル群構造を同じ方法でまとめて作ることができます。しかも方法は双曲線を用いた図形的には初等的に見えるものになります。

黒木玄 **Gen Kuroki** @genkuroki on May 6

円や楕円曲線のアーベル群構造について、楕円積分、対数、逆三角函数がすべて仲間であることについては以下のリンク先でも色々書きました。
mathtod.online/@genkuroki/3533...
mathtod.online/@genkuroki/3831...
mathtod.online/@genkuroki/2976...

黒木玄 **Gen Kuroki** @genkuroki on May 6

exp、sin、Jacobiのsn函数の加法公式はどれも

$$\begin{aligned}\int_{(x_0,y_0)}^{(x_1,y_1)}\omega+\int_{(x_0,y_0)}^{(x_2,y_2)}\omega&=\int_{(x_0,y_0)}^{(x_3,y_3)}\omega,\\ x_3&=\varphi(x_1,y_1,x_2,y_2),\\ y_3&=\psi(x_1,y_1,x_2,y_2)\end{aligned}$$

の形に書き直せます。ここで (x,y) は平面曲線上の座標であり、$\int_{(x_0,y_0)}^{(x,y)}$ は曲線上の点 (x_0,y_0) から (x,y) までの曲線上の経路で、ω は曲線上の微分形式です。φ,ψ は x_1,y_1,x_2,y_2 の多項式または有理函数になります。

すでに400字を超えている！数式はあんまり書けないな。

黒木玄 **Gen Kuroki** @genkuroki on May 6

抽象的一般論だけだと意味不明なので例を説明。まずexpとlog.

例：$xy=1,(x_0,y_0)=(1,1),\omega=dx/x$ のとき

$$\int_{(x_0,y_0)}^{(x,y)}\omega=\int_1^x\frac{dx}{x}=\log x.$$

実はたったこれだけの式の中に双曲線 $xy=1$ のアーベル群構造が実質的にすでに使われてしまっています。

反比例の曲線 $xy=1$ については実質的に算数で習うのですが、そこにアーベル群構造が入っていることは残念ながら習わない。

アーベル群構造を $\oplus$ と書くと、単位元を $(1,1)$ としたときの双曲線 $xy=1$ のアーベル群構造は

$$(x_1,y_1)\oplus(x_2,y_2)=(x_1x_2,y_1y_2)$$

になります。これは本質的に基礎体の乗法群そのものです。

反比例型の双曲線 $xy=1$ に入る自然なアーベル群構造は基礎体の乗法群と本質的に同じ。続く

黒木玄 **Gen Kuroki** @genkuroki on May 6

続き

$y_i=1/x_i$ なので

$$\begin{aligned}&(x_1,1/x_1)\oplus(x_2,1/x_2)\\&\quad=(x_1x_2,1/(x_1x_2))\end{aligned}$$

と書いた方がわかりやすいと感じる人はいるかも。この式の本質的なのは $x_1,x_2\mapsto x_1x_2$ の部分(単純に掛け算しているだけの部分)だけです。

次に $\omega=dx/x$ について。この微分形式(微分形式を知らなければ高校レベルの「積分できる何か」という理解で十分)は、x を定数倍 ax で置き換える操作で不変です：

$$\frac{d(ax)}{ax}=\frac{a\,dx}{ax}=\frac{dx}{x}.$$

アーベル群構造は単純な掛け算だったので、$\omega=dx/x$ はアーベル群の作用によって不変な微分形式だということになります。このような微分形式は定数倍を除いて一意に定まります。

これで $\omega=dx/x$ が必然的にどのように出て来るかもわかりました。

大抵の場合、群の作用で不変なものが大事になります。

黒木玄 **Gen Kuroki** @genkuroki on May 6

$\exp$ は

$$\log x=\int_1^x\frac{dx}{x}$$

の逆函数なので$\exp(u_1+u_2)=\exp(u_1)\exp(u_2)$ は $x_i=\exp(u_i)$ と置くことによって、

$$\log x_1+\log x_2=\log(x_1x_2)$$

と書き直されます。さらにこれは

$$\int_1^{x_1}\frac{dx}{x}+\int_1^{x_2}\frac{dx}{x}=\int_1^{x_1x_1}\frac{dx}{x}$$

と同値。そして、これは dx/x が群作用で不変なことを使って証明できます。左辺の後者の積分で x を x_1x で置換すると、dx/x の部分は不変で積分範囲だけが変化します：

$$\int_1^{x_2} \frac{dx}{x} = \int_{x_1}^{x_1 x_2} \frac{dx}{x}.$$

あとは

$$\int_1^{x_1} + \int_{x_1}^{x_1 x_2} = \int_1^{x_1 x_2}$$

を使えば積分和に関する上の公式が得られます。

黒木玄 **Gen Kuroki** @genkuroki on May 6

続き。このように、$\log$ や $\exp$ の背景には算数で習う反比例型の双曲線 $xy = 1$ が隠れています。

算数では習わない双曲線 $xy = 1$ のアーベル群構造(実は基礎体の乗法群と本質的に同じ)から、不変微分形式 $\omega = dx/x$ が得られ、 $\log$ が不定積分で定義され、その逆函数で $\exp$ が定義され、アーベル群構造をもとにして作った函数なのでそれらは自然に加法公式を満たすことになるわけです。

このストーリーを円 $x^2 + y^2 = 1$ に適用すると、$\omega = dy/y$ の不定積分として $\arcsin$ が得られ、その逆函数として $\sin$ が得られ、自然に三角函数の加法定理も得られます。

その計算を最初から最後まで遂行するのは高校数学の非常に良い復習になると思います。

最近の数学ファンは楕円曲線または楕円函数に詳しいという印象があるのですが、三角函数についても詳しくなっておくべきだと思います。

黒木玄 **Gen Kuroki** @genkuroki on May 6

まとめ：
(1)対数函数と指数函数の理論は曲線 $xy = 1$ に関する理論に含まれる。
(2) $\arcsin$ と $\sin, \cos$ の理論は曲線 $x^2 + y^2 = 1$ に関する理論に含まれる。

別の良い曲線に同じストーリーを適用すれば対数・指数函数、三角函数以外の有益な函数が得られるのではないか？

この問題への答えの一つが楕円曲線と楕円函数の理論です。アーベルさんとヤコビさんはとても偉いです。

ヤコビさんは楕円函数をテータ函数の商で書いたのですが、テータ函数は直接的な計算が易しく、色々いじりやすい函数なので私はとても気に入っています。テータ函数の理解は以上のストーリーより一段上の話になっていると思う。

最近、mathtodon のおかげで、テータ函数に関する標準的な文献であるMumord Tata Lectures on Theta がすべて無料でダウンロード可能になっていることに気付きました。
mathtod.online/@genkuroki/3044...