黒木玄 **Gen Kuroki** @genkuroki on May 1

三角函数や楕円函数が加法公式を持つ理由については様々な見方があります。

楕円函数に関してはアーベルさんによるオリジナルの議論についてはツイッターで詳しく紹介しました。
twitter.com/i/moments/84925504...

しかし、そこで紹介してある三角函数のケースは分かり易くない。

大雑把に言えば、代数的にアーベル群構造が入る曲線があればその曲線をパラメトライズする函数は加法公式を満たします。

例えば、円には純粋に代数(幾何)的にアーベル群構造が入ります。(より一般に円錐曲線にアーベル群構造が入る。)

円のアーベル群構造は二本の平行な直線を考えれば構成できます。さらに別の同値な方法として双曲線を使ってアーベル群構造を構成する方法もあります。
twitter.com/i/moments/85723103...

続く

黒木玄 **Gen Kuroki** @genkuroki on May 1

続き

で、円に双曲線を使ってアーベル群構造を入れる方法はそのまま楕円曲線に一般化されます。ただし、楕円曲線の標準形として次のEdwards形式を選ぶ。

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

a=0の場合が円の場合です。
twitter.com/i/moments/85598129...

Edwards曲線から自然に得られる楕円函数の加法公式はJacobiのcd函数とsn函数の加法公式です。それぞれ円の場合にcosとsinに対応する。
twitter.com/i/moments/85635943...

その加法公式はWeierstrass formの場合よりもシンプルでコンピューターでの効率的な計算に向いています。(Weierstrass formの場合には双曲線ではなく、直線で加法構造を構成する。)

この事実は楕円曲線暗号に応用されています。 Ed25519についてググればわかります。

続く

黒木玄 **Gen Kuroki** @genkuroki on May 1

続き

以上では(ツイッターでは)、わざと具体的な計算に帰着できるように説明したのですが、座標系に依存しない見方の方が数学畑では詳しい人が多いと思います。

楕円函数の加法公式は楕円曲線が自然にアーベル群構造を持つことの言い直しになっています。

そして、任意の曲線にはアーベル群であることが自明な群が付随しています。それは因子類群です。楕円曲線の場合には次数0の因子類群との同型によって群構造が入るわけです。

円(より一般に円錐曲線)の場合にも楕円曲線の場合にも直線(達)や双曲線との交わりが定める因子を計算することによって計算力にあまり頼らずに群になることを証明できます。

こういう代数幾何における基本的な道具のありがたみは楕円函数論を勉強して計算に苦労していればものすごく納得できるようになります。

黒木玄 **Gen Kuroki** @genkuroki on May 1

私のツイッターでの数学関係の雑談は
twitter.com/i/moments/84495913...
にまとめがあります。

あとmathtodonでの「初期」に書いたものについては
mathtod.online/@genkuroki/3229...
にまとめがあります。

黒木玄 **Gen Kuroki** @genkuroki on May 1

Edwards曲線としての楕円曲線については
mathtod.online/@genkuroki/2991...
にも書いた。

黒木玄 **Gen Kuroki**
@genkuroki

円のアーベル群構造は非常にシンプルで簡単な話です。

まず、円のアーベル群構造 $\oplus$ は三角函数を使えば

$$\begin{aligned}&(\cos\alpha,\sin\alpha)\oplus(\cos\beta,\sin\beta)\\&=(\cos(\alpha+\beta),\sin(\alpha+\beta))\end{aligned}$$

で簡単に定義できます。しかし、この定義から三角函数の加法公式を出そうとするのは苦しい。

円のアーベル群構造を超越函数に頼らずに多項式や有理函数程度の計算で構成したい。

答えは添付画像の図の二本の直線と円の交わりを使う方法です。
twitter.com/genkuroki/status/8...

続く

mathtod.online/media/GDmVMd5UQ...

2017年05月01日 20:49 · Web · 1 · 2 · Webで開く

黒木玄 **Gen Kuroki** @genkuroki on May 1

続き。その図では点 $O=(1,0)$ が単位元で、点 A と B の和を直線 AB と平行な点 O を通る直線と円の交点と定めることによって円のアーベル群構造は三角関数に頼らない方法で定義できます。

画像を見れば角度的にも和になっていることがすぐにわかりますが、角度のような概念を一切使わずにアーベル群構造が定義されています。(図は実数体上の曲線のつもりで書いていますが、実数体でなくてもすべて同じ計算になる。しかも、アフィン変換で不変な計算になっている。)

$A=(x_1,y_1), B=(x_2,y_2)$ のとき A と B の和を中学生レベルの方法で計算すると $(x_1x_2-y_1y_2, x_1y_2+x_2y_1)$ になることがわかります。これは三角函数の加法公式の導出にもなっています。

要するに純代数的な方法で超越函数の加法公式を導出できるわけです。

黒木玄 **Gen Kuroki** @genkuroki on May 1

続き。で、三角函数のような超越函数がどのようにしてx^2+y^2=1のような代数的に定義された曲線から得られるのか？

$$\omega=\frac{dy}{x}=\frac{y}{\sqrt{1-y^2}}$$

の積分で定義される函数

$$\theta(y) = \int_0^y \frac{dy}{\sqrt{1-y^2}}$$

を考えます。速さの積分で曲線の長さが表わされるという高校数学IIIで習う結果を使うと、$\theta(y)$ がラジアンの意味での角度であることがわかります。角度 $\theta = \theta(y)$ における y 座標が $y = y(\theta)$ が高校で習う $\sin$ の定義でした。すなわち、$y = \sin\theta$ は積分で定義された函数 $\theta = \theta(y)$ の逆函数です。

曲線上の被積分函数(微分形式) ω さえ与えられれば、その不定積分の逆函数でいつでも意味ありげな函数を定義できます。

続く

黒木玄 **Gen Kuroki** @genkuroki on May 1

続き

上の $\omega = dy/x$ を適切に円全体に拡張したものは円上の特別な被積分函数 (1-form)になっています。

円には純代数的な中学校レベルの計算でアーベル群の構造が最初から入っています。

そのアーベル群の構造に関する「平行移動」で上の ω は不変な微分形式になっています。

そこら辺のことをしっかり考えると、ω の不定積分の逆函数として定義された $\sin$ (および $\cos$)が、純代数的で中学校レベルの計算で構成された加法公式と同じ公式を満たしていることが計算無しで出て来ます。

このようにして三角函数の加法公式を証明することもできるわけです。遠回りなのですが、この方法はそのまま楕円曲線まで一般化されます。

この手の話は19〜20世紀にかけて相当に徹底的に研究されています。私にとっては完全に専門外なのですが。