P−14

虚数乗法と Kronecker の青春の夢
Complex Multiplication and Kronecker's Jugendtraum

○寺島三晴[1], 上石冬華[1] , 吉崎哲也[1] , 佐々木隆二[2]
Mitsuharu Terashima[1], Fuyuka Kamiishi[1], Tetsuya Yoshizaki[1], Ryuji Sasaki[2]

Abstract
Cyclotomic fields are abelian extesions over $\mathbb{Q}$ and conversely finite abelian extensions of $\mathbb{Q}$ are subfields of cyclotomic fields. Kronecker studied finite abelian extension of an imaginary quadratic field and he dreamed to prove the above theorem over imaginary quadratic fields.
In this talk, we explain an abelian extension of $\mathbb{Q}(i)$ by using an elliptic curve with complex multiplication.

1　Kronecker-Weber の定理

有理数体 $\mathbb{Q}$ に 1 の原始 n 乗根 ζ を添加した代数体 $\mathbb{Q}(\zeta)$ を円分体と呼ぶ. 円分拡大は有限アーベル拡大である.

この円分体の良い性質として, 次の定理が成り立つ.

Th. $\mathbb{Q}$ の任意の有限アーベル拡大体 F に対し, ある円分体 $\mathbb{Q}(\zeta)$ が存在し, 次を満たす.

$$F \subset \mathbb{Q}(\zeta).$$

この定理は, 有理数体の全ての有限アーベル拡大は円分体に含まれる事を意味している. これを発展させて, 基礎体 $\mathbb{Q}$ を虚二次体, 即ち $\mathbb{Q}(i)$ 等の $\mathbb{Q}$ の二次拡大で実数体 $\mathbb{R}$ に含まれない体, に置き換えても似た命題が成り立つのではないか, という予想を Kronecker は立てた.

ここでは, その一つの例として $\mathbb{Q}(i)$ の場合を考え, 1 の原始 n 乗根に対応するものとして楕円曲線の等分点を用いた拡大を定義する.

2　虚数乗法

以降, 楕円曲線とは有理係数楕円曲線の事である. 有理係数楕円曲線とは次の事である.

Def. a, b, c を有理数とする. この時, 次の曲線 C を有理係数楕円曲線と呼ぶ.

$$C\colon y^2 = x^3 + ax^2 + bx + c.$$

ここで, $x^3 + ax^2 + bx + c = 0$ は重根を持たないとする.

曲線 C 上の点の集合を $C(\mathbb{C})$ （無限遠点も含むとする）と表記する. $C(\mathbb{C})$ に和を適当に定めれば, これは群を成す.[1, pp28-32]

$C(\mathbb{C})$ の自己準同型写像 $\lambda_n(P) = nP$ を n 倍写像と呼ぶ.

$C(\mathbb{C})$ の自己準同型写像で n 倍写像でないものを虚数乗法と呼ぶ. ここでは, なぜ虚数乗法と呼ばれるのかを述べる.

楕円曲線は, $L := \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ $(\omega_1, \omega_2 \in \mathbb{C})$ を適当に定めれば $C(\mathbb{C}) \simeq \mathbb{C}/L$ である.

故に, 準同型 ϕ に対応して 0 の近傍から 0 への関数 f が存在する.

実は f は正則である. 正則ゆえに, 0 の近傍上で,

$$f(z) = \sum_{n=0}^{\infty} c_n z^n$$

と表せる. f は準同型である事から,

$$f(z_1 + z_2) - f(z_1) - f(z_2) \in L$$

が導かれる. 故に $f(0) = c_0 \in L$ となる. この時, $\mathbb{C}/L$ との兼ね合いにより, $f(0) = 0$ としても良い.

これらを用いると, ある $c \in \mathbb{C}$ が存在し,

$$f(z) = cz$$

が成り立つ事が分かり, f を $\mathbb{C}$ 上の関数として定義できる.

この事から, 乗法という名前が付く事は自然であろう. 更に, ϕ が n 倍写像でないならば, この c は実数でない事が分かる. 故に虚数乗法という名前が付けられた.

3　楕円曲線とガロア理論

$K/\mathbb{Q}$ をガロア拡大とし, 以下を定義する.

Def. $C(K)$ を, 座標が K の元である $C(\mathbb{C})$ の部分集合と定義する. 更に, $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, $P = (x, y) \in C(K)$ に対し, $\sigma(P) = (\sigma(x), \sigma(y))$ と定義する.

このように定義すると, $C(K)$ が $C(\mathbb{C})$ の部分群となり, $\mathrm{Gal}(K/\mathbb{Q})$ は $C(K)$ に作用する. 更に, σ を $C(K)$ の写像とみなすと準同型になっている.

次に, $C[n]$ を n 倍写像 λ_n の核 $\ker(\lambda_n)$ として定める. 核である事から $C[n]$ は群であり, 実は次の関係が成り立つ.

$$C[n] \simeq \frac{\mathbb{Z}}{n\mathbb{Z}} \oplus \frac{\mathbb{Z}}{n\mathbb{Z}}.$$

$C[n]$ の大事な性質として, 次の命題が成り立つ.

[1]日大理工・院（前）・数学
[2]日大理工・教員・数学

Prop. $P=(x,y)$ が $C[n]$ の元であるならば, x,y は $\mathbb{Q}$ 上代数的である. 更に, $\mathbb{Q}$ に $C[n]$ の全ての元の座標を添加して得られた体を $\mathbb{Q}(C[n])$ とすると, この体は $\mathbb{Q}$ 上ガロア拡大である.

この $C[n]$ を用いて Kronecker の青春の夢を論じる.

4　ガロア表現

$C[n]$ は $\frac{\mathbb{Z}}{n\mathbb{Z}}\oplus\frac{\mathbb{Z}}{n\mathbb{Z}}$ と同型である事から, 基底 P_1,P_2 が存在する. 故に, $C[n]$ 上の準同型 h は $h(P_1),h(P_2)$ で特徴付けられる. 従って,

$$h(P_1)=\alpha_h P_1+\gamma_h P_2$$
$$h(P_2)=\beta_h P_1+\delta_h P_2$$

である時, 次のように行列を定める.

$$M_h=\begin{pmatrix}\alpha_h & \beta_h\\ \gamma_h & \delta_h\end{pmatrix}.$$

この時, $C[n]$ 上の準同型 g,h に対し,

$$M_{g\circ h}=M_gM_h$$

が成り立つ.

$\sigma\in\mathrm{Gal}(\mathbb{Q}(C[n])/\mathbb{Q})$ は $C[n]$ からの写像とみなすと, 実は $C[n]$ 上の自己同型写像になっている.

従って, σ から行列 M_σ が定まる. σ が同型である事から, M_σ は正則である. 故に, 次の写像

$$\rho_n\colon \mathrm{Gal}(\mathbb{Q}(C[n])/\mathbb{Q})\to \mathrm{GL}_2\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right),\ \sigma\mapsto M_\sigma$$

が定義できる. これは単射準同型である.[1, pp195-196]

5　Kronecker の青春の夢

ここで扱うのは, $\mathbb{Q}(i)$ の有限アーベル拡大である. 使用する楕円曲線は,

$$C\colon y^2=x^3+x$$

である. この曲線は次の虚数乗法を持つ.

$$\phi\colon C\to C,\ \phi(x,y)=(-x,iy).$$

$\mathbb{Q}(i)$ が「良い」体である所以の一つとして, 次の性質を持つ.

任意のガロア拡大 $K/\mathbb{Q}(i)$ に対し, $\sigma\in\mathrm{Gal}(K/\mathbb{Q}(i))$ と $P\in C(K)$ をとると,

$$\sigma(\phi(P))=\phi(\sigma(P))$$

が成り立つ. この性質を利用すると, 次の定理が示される.

Th. $K_n:=\mathbb{Q}(i)(C[n])$ は $\mathbb{Q}(i)$ 上アーベル拡大である.

この定理の証明の核心は, $\mathrm{Gal}(K_n/\mathbb{Q}(i))$ がアーベル群である事の証明である. その流れを述べる.

$\mathrm{Gal}(K_n/\mathbb{Q}(i))$ の元 σ は, ρ_n を用いて行列 $\rho_n(\sigma)=\begin{pmatrix}\alpha_\sigma & \beta_\sigma\\ \gamma_\sigma & \delta_\sigma\end{pmatrix}$ を定める.

一方, 虚数乗法 ϕ は $C[n]$ の自己準同型写像を定め, 故に行列 $A=M_\phi=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ を定める.

更に, $\mathbb{Q}(i)$ の良い性質より,

$$\sigma(\phi(P))=\phi(\sigma(P)).$$

である. $P=P_1,P_2$ とする事により, 次の式が導かれる.

$$\rho_n(\sigma)A=A\rho_n(\sigma).$$

この式により, 以下の補題を用いるとアーベル群である事が示される.

Lem 1.

(a) $A\in\mathrm{GL}_2\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)$.

(b) n の任意の素因数を l とすると, A は mod l でスカラー行列でない. これは, 以下のいずれかが成り立つ事を意味する.

(1) $b\not\equiv 0 \pmod{l}$;

(2) $c\not\equiv 0 \pmod{l}$;

(3) $a\not\equiv d \pmod{l}$.

Lem 2. $\left\{B\in\mathrm{GL}_2\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)\,|AB=BA\right\}$ はアーベル群.

この補題の証明に, 更に二つの補題を用いる.

Sublem 2'. A を $\mathrm{GL}_2\left(\frac{\mathbb{Z}}{l^e\mathbb{Z}}\right)$ の元とみなす. この時, 基底の変換行列 $T\in\mathrm{GL}_2\left(\frac{\mathbb{Z}}{l^e\mathbb{Z}}\right)$ が存在し, A を次のような標準形にする.

$$T^{-1}AT=\begin{pmatrix}0 & *\\ 1 & *\end{pmatrix}.$$

Sublem 2". $A=\begin{pmatrix}0 & *\\ 1 & *\end{pmatrix}\in\mathrm{GL}_2\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)$ とする.

この時, $\left\{B\in\mathrm{GL}_2\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)\,|AB=BA\right\}$ はアーベル群.

以上によって定理は証明される.[1, pp205-211] 最後に Kronecker の青春の夢を $\mathbb{Q}(i)$ の場合で記述して終りにする.

Th (Kronecker's Jugendtraum)**.** *[1, p211]* F を $\mathbb{Q}(i)$ の任意の有限アーベル拡大とする. この時, ある整数 n が存在して, 以下が成り立つ.

$$F\subset\mathbb{Q}(i)(C[n]).$$

参考文献

[1] J. H. Silverman & John Tate : "Rational Points on Elliptic Curves", Springer-Verlag UTM, 1992.