楕円曲線と立方数

渡　辺　　透

1．はじめに

Modell-Weil の定理の証明の中で定義される準同型写像 ϕ は，楕円曲線と平方数と間に密接な関係があることを示している。我々は，ある楕円曲線に対して同様の写像を定義することによって，立方数に対しても類似の関係を示すことができた。また，応用として，その証明の中で得られた恒等式によって，

$$X^3+Y^3+Z^3+W^3=0$$

に対する整数解の発見法を得ることができた。

2．Modell-Weil の定理の証明の流れ

まず，Modell-Weil の定理：『楕円曲線の有理点全体のなすアーベル群は有限生成である』の証明のポイントを振り返ってみよう。

楕円曲線を

$$E：y^2=x^3+ax^2+bx+c=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$$

とする。方法は同じなので，$\alpha_i\in\mathbf{Z}$ として示す。

STEP 1

$\beta：\mathbf{Q}^\times\to\mathbf{Q}^\times/\mathbf{Q}^{\times 2}=:G$　　を自然な写像とする。

$P\in E(\mathbf{Q})$ に対し，

$$\phi_i(P)=\begin{cases}1 & \text{if}\quad P=\mathcal{O}\\ \beta((x(P)-\alpha_j)(x(P)-\alpha_k)) & \text{if}\quad P=\alpha_i,\ \alpha_i\neq\alpha_j,\ \alpha_k\\ \beta(x(P)-\alpha_i) & \text{その他}\end{cases}$$

として，$\phi：E(\mathbf{Q})\to G\times G\times G$

$$P\mapsto(\phi_1(P),\ \phi_2(P),\ \phi_3(P))$$

と定義するとこれが群準同型になる。

STEP 2

$\ker\phi = 2E(\mathbf{Q})$

STEP 3

$\mathrm{Im}\phi$：finite （実際イメージに現れるのは判別式を割る素数のみ）

STEP 4

その後 height などを使い証明される。

これが典型的な証明の流れである。

3. 定　　理

ここで，$E: y^2+ay=x^3$ $(a\in\mathbf{Z})$ という楕円曲線を考えよう。

そこで，$\gamma: \mathbf{Q}^\times \to \mathbf{Q}^\times/\mathbf{Q}^{\times 3} =: H$ を自然な写像とし，

$$\psi_1(P)=\begin{cases} 1 & \text{if} \quad P=\mathcal{O} \\ \gamma(y(P)+a)^2 & \text{if} \quad y(P)=0 \\ \gamma(y(P)) & \text{その他} \end{cases}$$

$$\psi_2(P)=\begin{cases} 1 & \text{if} \quad P=\mathcal{O} \\ \gamma(y(P))^2 & \text{if} \quad y(P)=-a \\ \gamma(y(P)+a) & \text{その他} \end{cases}$$

と，定義して，

$$\begin{array}{ccccc} \psi: E(\mathbf{Q}) & \to & H & \times & H \\ P & \to & (\psi_1(P), & \psi_2(P)) & \end{array}$$

と，定義する。

定理 ψ は，群準同型である。

証明）

$P(x, y)\in E(\mathbf{Q})$ とすると，

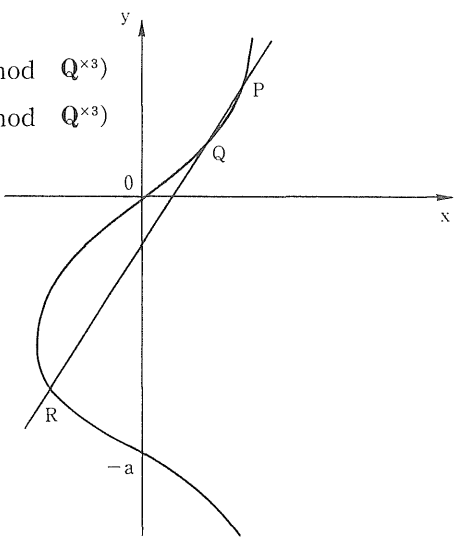
$$2P=\left\{\frac{x^4-2a^2x}{(2y+a)^2}, \frac{(-a+y)^3(a+y)}{(2y+a)^3}\right\}$$

である。よって，

$$\begin{aligned} \psi_1(2P) &\equiv (-a+y)^3(a+y) && (\mathrm{mod}\ \ \mathbf{Q}^{\times 3}) \\ &= (a+y) && (\mathrm{mod}\ \ \mathbf{Q}^{\times 3}) \\ &\equiv y^2 && (\mathrm{mod}\ \ \mathbf{Q}^{\times 3}) \\ &\equiv \psi_1(P)^2 && (\mathrm{mod}\ \ \mathbf{Q}^{\times 3}) \end{aligned}$$

また，

$$y(2P)+a=y(2a+y)^3 \equiv (y+a)^2 \equiv \psi_2(P)^2 \pmod{\mathbf{Q}^{\times 3}}$$



今，$P(x_1, y_1)$，$Q(x_2, y_2)$，$R(x_3, y_3)$ を E 上にある同一直線上の 3 点で，$y_1y_2y_3 \neq 0$ とすると，計算により，

$$y_1y_2y_3 \equiv 1 \pmod{\mathbf{Q}^{\times 3}}$$

が示される。$a(\neq 0)$ は任意だから，$E' : y^2-ay=x^3$ および $P'(x_1, y_1+a)$，$Q'(x_2, y_2+a)$，$R'(x_3, y_3+a)$ を考えることにより，

$$(y_1+a)(y_2+a)(y_3+a) \equiv 1 \mod \mathbf{Q}^{\times 3}$$

もいえる。$P+Q=(x', y')$ とすると，

$y'+y_2=-a$ だから　$y_1y_2(-a-y') \equiv 1 \pmod{\mathbf{Q}^{\times 3}}$

$\therefore\ y_1y_2 \equiv (y'+a)^2 \pmod{\mathbf{Q}^{\times 3}}$

$\equiv y' \equiv \psi_1(P+Q) \pmod{\mathbf{Q}^{\times 3}}$

同様に　$(y_1+a)(y_2+a) \equiv (y'+a) \pmod{\mathbf{Q}^{\times 3}}$

$\equiv \psi_2(P+Q) \pmod{\mathbf{Q}^{\times 3}}$

証明終

ただし，Modell-Weil の定理の証明の STEP 2 に相当する $\mathrm{Ker}\ \psi = 3E(\mathbf{Q})$ は成立しないので，この定理を使ってこの形の楕円曲線に限る別証明と与えることは難しいであろう。

4. 応　　用

ここで，

$$3P=\left[\frac{a^6+3a^4x^3-24a^2x^6+x^9}{\{3x(a^2+x^3)\}^2},\ \frac{(-a^3-4ax^3-2a^2y+x^3y)^3}{\{3x(a^2+x^3)\}^3}\right]$$

であって，$y(3P)$ および，

$$y(3P)+a=\frac{(-a^3+3a^2y+6ay^2+y^3)^3}{\{3x(a^2+x^3)\}^3}$$

という二つの立方数の関係から，次の恒等式が得られる。

$$(-a^3-4ax^3-2a^2y+x^3y)^3+a\{3x(a^2+x^3)\}^3=(-a^3+3a^2y+6ay^2+y^3)^3$$

たとえば，$a=7=2^3-1^3$ とすれば，点 $(2, 1)$ が曲線上にあることにより，

$$-73^3+(2^3-1^3)\cdot 38^3=-17^3$$

すなわち，

$$17^3+76^3=73^3+38^3$$

が得られる。このようにaを“立方数±立方数”として，楕円曲線E：$y^2+ay=x^3$の有理数解を求めれば，

$$X^3+Y^3+Z^3+W^3=0$$

の自明でない整数解が得られる。

a	x	y	X	Y	Z	W
7	2	1	−73	76	−38	17
9	−2	−1	−271	−876	−438	919
19	6	8	−27323	31158	−20772	−9613
26	3	1	−21709	18981	−6327	15391
28	−3	−1	−17333	−20439	−6813	24137
35	−6	−8	8693	−54486	−36324	59347
37	12	27	−333667	445968	−334476	−241757
61	20	64	−238141	390700	−312560	−249859
63	4	1	−274049	193584	−48396	237761
65	−4	−1	−27719	−22192	−5548	31879
91	−12	−27	369251	−943632	−707724	1045981
91	30	125	−9276821	19051740	−15876450	−12836179
98	15	27	−2691683	2920275	1752165	−285067

参考文献

A. W. Knapp: Elliptic Curves,Princeton

J. P. Serre: Introduction to Modell-Weil Theorem, Fried. Vieweg & Sohn, Braunshweig, 2nd edition, 1990.