楕円関数論 (11)
Weierstrass の楕円関数 (3) : 加法定理と楕円曲線

緒方　秀教

電気通信大学　大学院情報理工学研究科 情報・ネットワーク工学専攻

2020 年 12 月 31 日（木））

（まとめ）Weierstrass の楕円関数

周期格子

$(\omega_1, \omega_2 \in \mathbb{C} - \{0\},\ \mathrm{Im}(\omega_2/\omega_1) > 0)$

$$\Lambda = \{ m\omega_1 + n\omega_2 \mid m, n \in \mathbb{Z} \}.$$

Weierstrass の $\wp$ 関数

$$\wp(u) = \frac{1}{u^2} + \sum_{\omega \in \Lambda - \{0\}} \left(\frac{1}{(u-\omega)^2} - \frac{1}{\omega^2} \right).$$

- 2 位の楕円関数.

$$\wp(u + \omega_j) = \wp(u) \quad (j = 1, 2).$$

- $u = \omega \in \Lambda$ に 2 位の極.
- 偶関数.

（まとめ）Weierstrass の楕円関数

Weierstrass の zeta 関数

$$\zeta(u) = \frac{1}{u} + \sum_{\omega \in \Lambda - \{\,0\,\}} \left(\frac{1}{u-\omega} + \frac{1}{\omega} + \frac{u}{\omega^2} \right).$$

- 全複素平面 $\mathbb{C}$ で有理型関数．$u = \omega \in \Lambda$ に 1 位の極．
- 奇関数．
- 擬周期性．

$$\zeta(u+\omega_j) - \zeta(u) = \eta_j, \quad \eta_j = 2\zeta\left(\frac{\omega_j}{2}\right) \quad (j = 1, 2\,).$$

- $\zeta'(u) = -\wp(u)$.
- Legendre の関係式．

$$\eta_1\omega_2 - \eta_2\omega_1 = 2\pi\mathrm{i}.$$

（まとめ）Weierstrass の楕円関数

Weierstrass の sigma 関数

$$\sigma(u) = u \prod_{\omega \in \Lambda - \{\,0\,\}} \left(1 - \frac{u}{\omega}\right) \exp\left(\frac{u}{\omega} + \frac{u^2}{2\omega^2}\right).$$

- 全複素平面 $\mathbb{C}$ で整関数．$u = \omega \in \Lambda$ に 1 位の零点．
- 奇関数．
- 擬周期性．

$$\sigma(u + \omega_j) = -\exp\left(\eta_j \left(u + \frac{\omega_j}{2}\right)\right) \sigma(u) \quad (j = 1, 2\,).$$

- $\dfrac{\mathrm{d}}{\mathrm{d}u} \log \sigma(u) = \dfrac{\sigma'(u)}{\sigma(u)} = \zeta(u).$
- テータ関数による表現→数値計算．

$$\sigma(u) = \frac{\omega_1}{\vartheta_1'} \exp\left(\frac{\eta_1}{2\omega_1} u^2\right) \vartheta_1\left(\frac{u}{\omega_1} \middle| \tau\right) \quad \left(\tau = \frac{\omega_2}{\omega_1}\right).$$

今回の内容

- （Jacobi の楕円関数では加法定理があった）
  Weierstrass の楕円関数論にも**加法定理**がある.
- 楕円関数をシグマ関数で表示する式→ $\wp(u)$ に対する加法定理.
- **楕円曲線論**との関連.

楕円関数の sigma 関数による表現

定理

- $f(u)$：n 位の楕円関数（周期 ω_1, ω_2, $\mathrm{Im}(\omega_2/\omega_1) > 0$）.
- $a_1, \ldots, a_n \mod \Lambda$：$f(u)$ の零点,
  $b_1, \ldots, b_n \mod \Lambda$：$f(u)$ の極
  （多重度分繰り返し記す）.

$$a_1 + \cdots + a_n - (b_1 + \cdots + b_n) = \omega \in \Lambda$$

が成り立つので，$b_n + \omega \to b_n$ と置き換えることにより，

$$a_1 + \cdots + a_n = b_1 + \cdots + b_n$$

であると仮定する.

このとき,

$$f(u) = C\frac{\sigma(u-a_1)\cdots\sigma(u-a_n)}{\sigma(u-b_1)\cdots\sigma(u-b_n)} \quad (\ C\ :\ \text{const.}\ )$$

楕円関数の sigma 関数による表現

（証明）

$$g(u) = \frac{\sigma(u-a_1)\cdots\sigma(u-a_n)}{\sigma(u-b_1)\cdots\sigma(u-b_n)}$$

とおく．$f(u)$ と $g(u)$ は同じ零点・極をもつ．

$\sigma(u)$ の擬周期性と $a_1+\cdots+a_n = b_1+\cdots+b_n$ より

$$\begin{aligned} g(u+\omega_j) &= \exp\left(\eta_j \sum_{i=1}^{n}\left(u-a_i+\frac{\omega_j}{2}\right) - \eta_j \sum_{i=1}^{n}\left(u-b_i+\frac{\omega_j}{2}\right)\right) g(u) \\ &= g(u) \quad (j=1,2) \end{aligned}$$

であるから，$f(u), g(u)$ は同じ周期を持つ楕円関数である．

よって，$f(u)/g(u)$ は極を持たない楕円関数であるから，定数関数である．

$$\frac{f(u)}{g(u)} \equiv \text{const.}$$

これで定理が証明された． ■

Weierstrass 楕円関数の加法定理 (1)

$$\wp(u) - \wp(v) = -\frac{\sigma(u-v)\sigma(u+v)}{\sigma(u)^2\sigma(v)^2}.$$

（証明）v を固定して考えると，
$\wp(u) - \wp(v)$ は 2 位の楕円関数で，$u \equiv 0 \mod \Lambda$ に 2 位の極を持ち，
$u \equiv \pm v \mod \Lambda$ に 1 位の極を持つ．そして，$v + (-v) = 0$ である．
よって，定理より

$$\wp(u) - \wp(v) = C\frac{\sigma(u-v)\sigma(u+v)}{\sigma(u)^2} \quad (\ \ C\ \ :\ \ \text{const.}\ \ ).$$

C を決めるために，両辺に u^2 を掛けて $u \to 0$ とすると，
$u = 0$ において $\wp(u) = u^{-2} + \mathrm{O}(u^2)$ であることに注意して

$$1 = C\sigma(-v)\sigma(v) = -C\sigma(v)^2, \quad C = -\frac{1}{\sigma(v)^2}.$$

ゆえに公式が証明された． ■

Weierstrass 楕円関数の加法定理 (1)

$$\begin{vmatrix} 1 & \wp(u) & \wp'(u) \\ 1 & \wp(v) & \wp'(v) \\ 1 & \wp(w) & \wp'(w) \end{vmatrix} = 2\sigma(u+v+w)\frac{\sigma(u-v)\sigma(v-w)\sigma(w-u)}{\sigma(u)^3\sigma(v)^3\sigma(w)^3}.$$

（証明）v, w を固定して左辺を u の関数とみなすと，これは 3 位の楕円関数で $u \equiv 0 \mod \Lambda$ に 3 位の極をもつ．

左辺は $u \equiv v, w \mod \Lambda$ に 1 位の零点を持ち，零点の個数=極の個数=3 より
もうひとつ 1 位の零点をもつが，$\sum$（零点）$\equiv \sum$（極）$= 0$ より
それは $-v - w$ である．よって定理より，

$$\text{左辺} = \text{const.} \times \frac{\sigma(u-v)\sigma(u-w)\sigma(u+v+w)}{\sigma(u)^3}$$

と書ける．u, v, w についての対称性を考えると，

$$\text{左辺} = C\sigma(u+v+w)\frac{\sigma(u-v)\sigma(v-w)\sigma(w-u)}{\sigma(u)^3\sigma(v)^3\sigma(w)^3} \quad (\ C\ :\ \text{const.}\ )$$

と書けるはずである．

Weierstrass 楕円関数の加法定理 (1)

定数 C を決めるために，両辺の $u=0$ における Laurent 級数展開を比べると，

$$
\begin{aligned}
\text{左辺} &= \begin{vmatrix} 1 & \wp(u) & \wp'(u) \\ 1 & \wp(v) & \wp'(v) \\ 1 & \wp(w) & \wp'(w) \end{vmatrix} = \begin{vmatrix} 1 & u^{-2}+\cdots & -2u^{-3}+\cdots \\ 1 & \wp(v) & \wp'(v) \\ 1 & \wp(w) & \wp'(w) \end{vmatrix} \\
&= 2\{\wp(v)-\wp(w)\}\frac{1}{u^3}+\cdots \\
&= -2\frac{\sigma(v-w)\sigma(v+w)}{\sigma(v)^2\sigma(w)^2}\frac{1}{u^3}+\cdots, \\
\text{右辺} &= C\frac{\sigma(v+w)\sigma(v-w)\sigma(-v)\sigma(w)}{u^3\sigma(v)^3\sigma(w)^3}+\cdots \\
&= -C\frac{\sigma(v-w)\sigma(v+w)}{\sigma(v)^2\sigma(w)^3}\frac{1}{u^3}+\cdots. \\
&\therefore \quad C=2.
\end{aligned}
$$

■

Weierstrass 楕円関数の加法定理 (1)

$\wp(u)$ の加法定理

$$\begin{vmatrix} 1 & \wp(u) & \wp'(u) \\ 1 & \wp(v) & \wp'(v) \\ 1 & \wp(w) & \wp'(w) \end{vmatrix} = 0 \quad \text{if} \quad u+v+w \equiv 0 \mod \Lambda.$$

これより，

$u+v+w \equiv 0 \mod \Lambda$ ならば，3 点

$$(\wp(u), \wp'(u)), \quad (\wp(v), \wp'(v)), \quad (\wp(w), \wp'(w))$$

は $\mathbb{C}^2$ 内で一直線上に並ぶ．

楕円曲線

楕円曲線

$\mathbb{C}^2$ 内の曲線

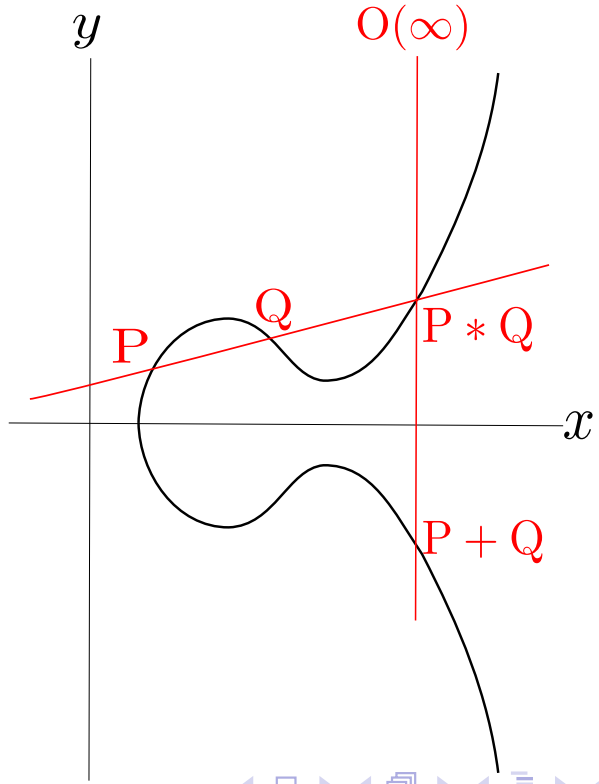
$$y^2 = 4x^3 - g_2 x - g_3 \quad (\, g_2^3 - 27 g_3^2 \neq 0\,).$$

$*$ より正確には，射影平面 $\mathbb{P}^2(\mathbb{C})$ 内の曲線.

楕円曲線上の点に対して，右図のように**加法（群演算）**

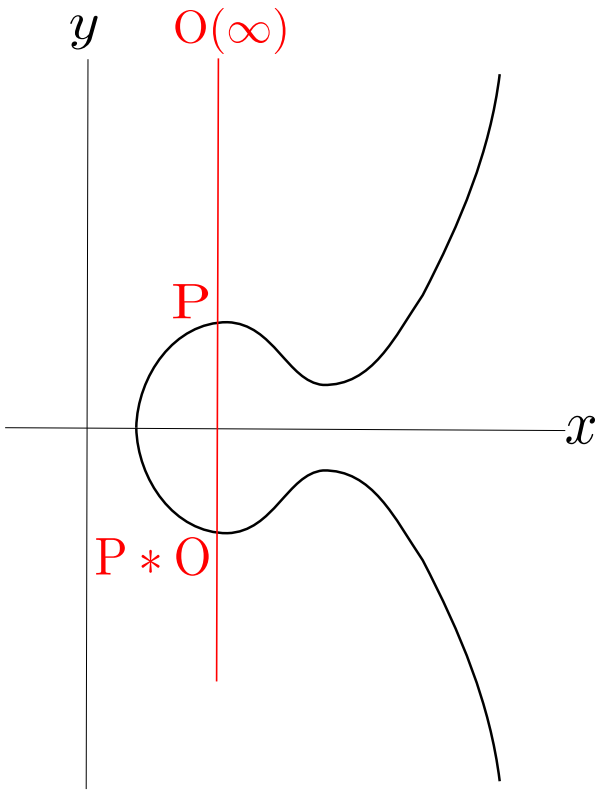
$$(\mathrm{P}, \mathrm{Q}) \mapsto \mathrm{P} + \mathrm{Q}$$

を定めることができる.

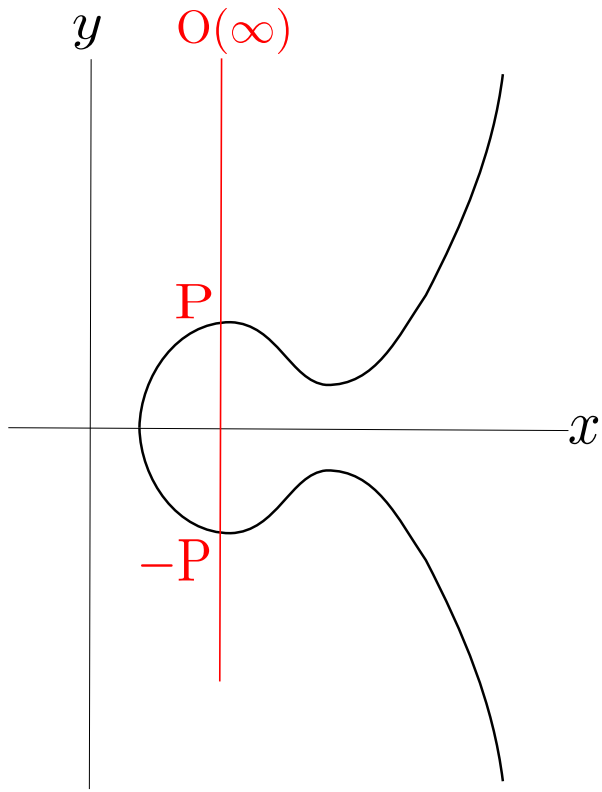


楕円曲線

楕円曲線上の加法は群の公理を満たす.



O（無限遠点）は単位元



逆元 −P

結合則：$(\mathrm{P}+\mathrm{Q})+\mathrm{R}=\mathrm{P}+(\mathrm{Q}+\mathrm{R})$（これを示すのは面倒）.

楕円曲線

$\wp(u)$ の満たす微分方程式.

$$\wp'(u)^2 = 4\wp(u)^3 - g_2\wp(u) - g_3.$$

楕円曲線のパラメータ表示

楕円曲線

$$y = 4x^3 - g_2x - g_3$$

は $\wp$ 関数でパラメータ表示される.

$$(x, y) = (\wp(u), \wp'(u)).$$

$*$ 与えられた g_2, g_3 に対し

$$g_2 = 60 \sum_{\omega \in \Lambda - \{0\}} \frac{1}{\omega^4}, \quad g_3 = 140 \sum_{\omega \in \Lambda - \{0\}} \frac{1}{\omega^6}$$

を満たす周期格子 Λ（周期 ω_1, ω_2）は存在する.

楕円曲線

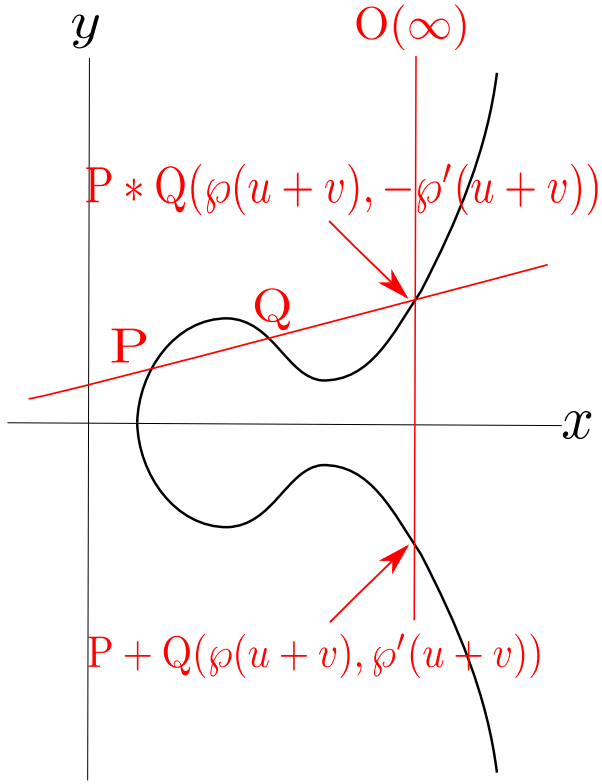
楕円曲線上の加法：
$\wp(u)$ の加法定理より

$$\begin{aligned} &\mathrm{P}(\wp(u), \wp'(u)), \\ &\mathrm{Q}(\wp(v), \wp'(v)), \\ &\mathrm{P} * \mathrm{Q}(\wp(u+v), -\wp'(u+v)) \end{aligned}$$

は一直線上にある.

$$\Downarrow$$

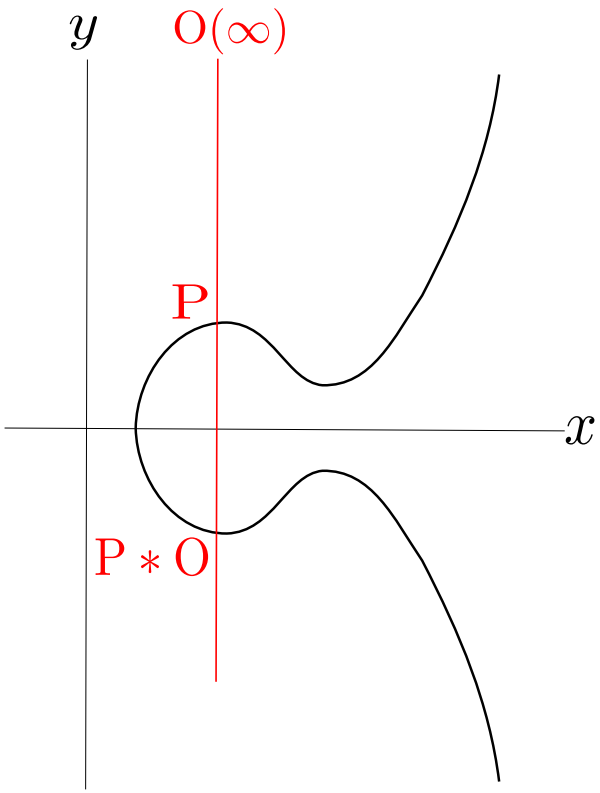
$$\mathrm{P} + \mathrm{Q} = (\wp(u+v), \wp'(u+v)).$$



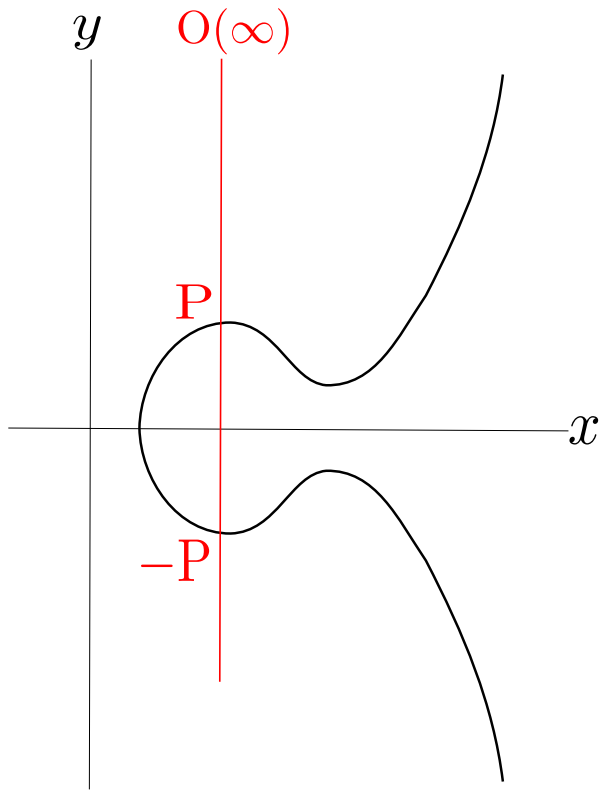
結合則（$\wp(u)$ でパラメータ表示すると自明）

$$\begin{aligned} (\mathrm{P} + \mathrm{Q}) + \mathrm{R} &= (\wp((u+v)+w), \wp'((u+v)+w)) \\ &= (\wp(u+(v+w)), \wp'(u+(v+w)) = \mathrm{P} + (\mathrm{Q} + \mathrm{R}). \end{aligned}$$

楕円曲線



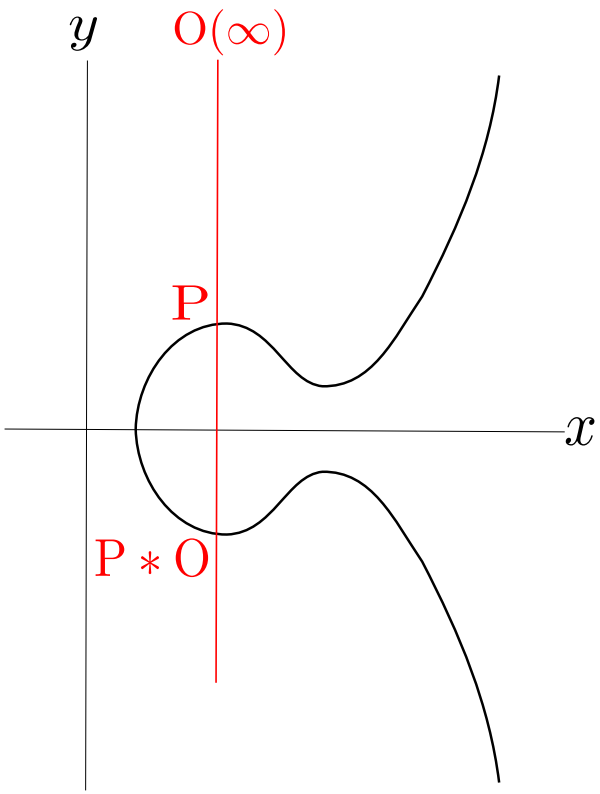
O（単位元）$\wp(0) = \infty$



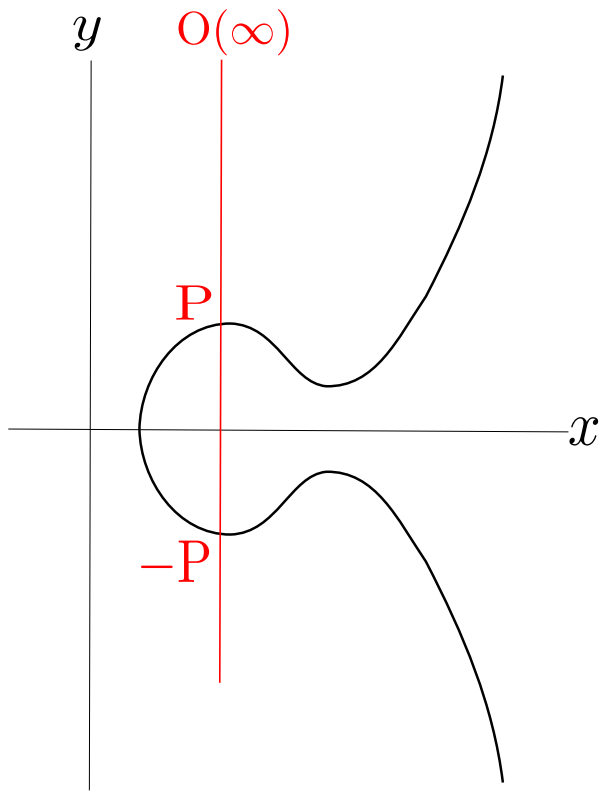
逆元 $-\mathrm{P}$

$(\wp(-u), \wp'(-u)) = (\wp(u), -\wp'(u))$

楕円曲線



O（単位元）$\wp(0) = \infty$



逆元 $-\mathrm{P}$

$(\wp(-u), \wp'(-u)) = (\wp(u), -\wp'(u))$

楕円曲線上の加法は，楕円関数によるパラメータ表示
$(x, y) = (\wp(u), \wp'(u))$ におけるパラメータの加法 $u + v$ に帰着される．

まとめ

- 楕円関数のシグマ関数による表現.
- $\wp(u)$ の加法定理.

$$\begin{vmatrix} 1 & \wp(u) & \wp'(u) \\ 1 & \wp(v) & \wp'(v) \\ 1 & \wp(w) & \wp'(w) \end{vmatrix} = 0 \quad \text{if} \quad u+v+w \equiv 0 \mod \Lambda.$$

- 楕円曲線論との関連.
  楕円曲線上の加法は $\wp(u)$ の引数の和に対応する.