平行光線による射影

3 次元空間を $\mathbb{R}^3$ と表わし，x, y, z 軸を考える．また，$\mathbb{R}^3$ の中の xy 平面は

$$H = \{(x, y, 0) | x, y \in \mathbb{R}\}$$

と表わされる．
空間内に方向 $\mathbf{v} = (p, q, r)$ $(r \neq 0)$ に平行な光線の束で，3 次元空間内の図形を H に投影することを考えよう．

$\mathbb{R}^3$ 上の点 $A = (x, y, z)$ を H に投影した点 B は，
$(x - pz/r, y - qz/r, 0)$ として与えられ，これを方向 $\mathbf{v}$ の**平行射影**と呼ぶ．
特に光線の方向が H と垂直なとき，すなわち $\mathbf{v} = (0, 0, 1)$ のとき，**正射影**と呼ぶ．

平行光線による射影

問題 4

点 B が $(x - pz/r, y - qz/r, 0)$ として与えられることを示せ.

点光源による射影

$\mathbb{R}^3$ 内の一点 $P = (p, q, r)$ に点光源を置いて，点 $A = (x, y, z)$, $(z \neq r)$ を H に投影した点 B は，$(\frac{zp-rx}{z-r}, \frac{zq-ry}{z-r}, 0)$ として与えられ，これを**点射影**と呼ぶ.

問題 5

点 B が $(\frac{zp-rx}{z-r}, \frac{zq-ry}{z-r}, 0)$ として与えられることを示せ.

点光源による射影

円錐曲線とは，円錐を平面で切ったときに現れる切り口の図形のことである．

定理 1

円錐曲線，すなわち楕円，放物線，双曲線は，点射影による単位円の像として得られる．

定理 1 の例

点 $(0,0,1)$ からの点射影を考えることにし，射影は

$$\pi : \mathbb{R}^3 \to \mathbb{R}^2, \pi((x,y,z)) = \frac{1}{1-z}(x,y)$$

と表され，射影できないような点の集合は平面 $z = 1$ であって，Ω で表す．次に，方程式 $x = 1$ で表される平面を

$$K = \{(1,y,z) : y,z \in \mathbb{R}\}$$

とし, K 上の単位円を射影 π によって xy 平面 H へと射影してみる．このとき円と平面 Ω の位置関係によって異なる図形に投影される．

定理１の例

円が Ω と交わらない場合 円を $x = 1, y^2 + (z-3)^2 = 1$ とするとき，**楕円**に射影される.

円が Ω と接している場合 円を $x = 1, y^2 + z^2 = 1$ とするとき，**放物線**に射影される.

円が Ω と２点で交わっている場合 円を $x = 1,$ $y^2 + (z-1)^2 = 1$ とするとき，**双曲線**に射影される.

点光源による射影

定理 2

平面上の平行な２直線は無限遠点で交わる.

共線，共点

平面あるいは空間内の直線の集合 $\mathcal{L} = \{l_1, l_2, \ldots\}$ が与えられたとき，$\mathcal{L}$ が**共点**であるとは，これらの直線がある一点で交わるときにいう．また点の集合 $\mathcal{P} = \{p_1, p_2, \ldots\}$ に対して，$\mathcal{P}$ が**共点**であるとは，$\mathcal{P}$ の点が同一直線上にあるときにいう．

デザルグの定理

定理 3 (平面版デザルグの定理)

平面上の 2 つの三角形 ΔABC と $\Delta A'B'C'$ の対応する頂点を結ぶ 3 本の直線 AA', BB', CC' が共点であるする. このとき，対応する辺を延長した直線同士の交点

$$P = AB \cap A'B', Q = BC \cap B'C', R = CA \cap C'A'$$

が存在すれば，それらは共線である.

空間版デザルグの定理

定理 4 (空間版デザルグの定理)

空間内の 2 つの三角形 ΔABC と $\Delta A'B'C'$ の対応する頂点を結ぶ 3 本の直線 AA', BB', CC' が共点であるする. このとき,

(1) 対応する辺を延長した直線同士は, 平行であるか一点で交わる.

(2) 3 組の対応する辺同士が交点を持てば, それら 3 つの交点は共線である. すなわち, 対応する辺を延長した直線同士の交点

$$P = AB \cap A'B', Q = BC \cap B'C', R = CA \cap C'A'$$

が存在すれば, それらは共線である.

(3) 2 組の対応する辺同士が平行ならば, 残りの 1 組も平行である

パップスの定理

定理 5 (パップスの定理)

平面上に 2 直線 l_1, l_2 があり，各直線 l_i $(i = 1, 2)$ 上に 3 点 A_i, B_i, C_i を取る．このとき，次の直線の交点 $P_1 = A_1B_2 \cap A_2B_1$, $P_2 = B_1C_2 \cap B_2C_1$, $P_3 = C_1A_2 \cap C_2A_1$ は共線である．

点の取り方によってはユークリッド平面上でパップスの定理が成り立たない場合があるが，射影平面として考えることで（平行な直線が無限遠点で交わると考えることで）パップスの定理の拡張として考えることができる．

射影平面

点光源を 3 次元空間 $\mathbb{R}^3$ の原点 $O = (0, 0, 0)$ とし，空間内の平面 K への射影 π を考える.
空間内の点 $\mathbf{x} = (x, y, z)$ の K への射影は，$\mathbf{x}$ と原点を結ぶ直線 l と平面 K との交点 X である.
このとき, 直線 l 上の点 $\mathbf{x}$ 以外の点 $\mathbf{x}'$ も射影 π によって同じ点 X に写される.
つまり $\mathbf{x}$, $\mathbf{x}'$ は平面 K 上の点 X と同一視することができる.
すなわち $\mathbb{R}^3$ 内の原点を通る直線一つずつを点とみなし，原点を通る直線の全体を射影平面 $(\mathbb{P}^2(\mathbb{R}))$ と捉えることができる.

射影平面：代数的表現

$\mathbf{x} = (x, y, z)$, $\mathbf{x}' = (x', y', z') \in \mathbb{R}^3 \setminus \{0\}$ に対し，

$$(x, y, z) \sim (x', y', z') \Leftrightarrow \exists \lambda \in \mathbb{R} \setminus \{0\} \text{ s.t. } (x, y, z) = \lambda(x', y', z')$$

と定義したとき，$\sim$ は同値関係をなし，この同値関係による商集合を**射影平面**という．
すなわち，$\mathbb{P}^2(\mathbb{R}) = \mathbb{R}^3 \setminus \{0\}/\sim$ である．

射影平面：代数的表現

(x, y, z) の属する同値類を $[x : y : z]$ と表し，これを射影平面上の点表現とする．
$z \neq 0$ となる点 (x, y, z) は，

$$(x, y, z) \sim (\frac{x}{z}, \frac{y}{z}, 1)$$

であるので，平面 $H_z : z = 1$ 上の点 $(X, Y, 1), (X = \frac{x}{z}, Y = \frac{y}{z})$ とみなすこともできる．これを**アフィン平面**という．また射影平面上において，$z = 0$ としたときの同値類の集まり (ただし $x = y = 0$ を除く) が **無限遠直線**となる．

射影平面：代数的表現

定理 10

射影平面 $\mathbb{P}^2(\mathbb{R})$ は,

$$\mathbb{P}^2(\mathbb{R}) = \{[X : Y : 1] : (X, Y) \in \mathbb{R}^2\} \cup \{[x : y : 0] : (x, y) \neq (0, 0)\}$$

で与えられる

射影平面を公理から

$\mathcal{P}$ を点集合 $\{p_1, p_2, \ldots\}$，$\mathcal{L}$ を直線の集合 $\{l_1, l_2, \ldots, \}$ とし，I を $\mathcal{P}$ と $\mathcal{L}$ の結合関係（直積集合 $\mathcal{P} \times \mathcal{L}$ の部分集合）とする．このとき $\mathcal{A} = (\mathcal{P}, \mathcal{L}, I)$ を**結合構造**という．

ここで点 p_i が $\mathcal{L}$ の部分集合 l_j に含まれるとき，p_i と l_j は結合関係 I にあるといい，$p_i I l_j$ と書く．幾何学的な表現を用いると，点 p_i は直線 l_j の**上にある**，直線 l_j は点 p_i を**通る**などという．

アフィン平面

アフィン平面とは，次の公理を満たす結合構造 $\mathcal{A} = (P, L, I)$ である．

(A1) 異なる２点を通る直線はただ一つ存在する．

(A2) 任意の直線 $l \in L$ と l 上にはない任意の点 p を与えたとき，p を通り l と交わらない直線 h がちょうど１つ存在する．

(A3) 同一直線上にない 3 点が存在する．

特に P と L が有限集合のとき，この結合構造を有限アフィン平面とよぶ．アフィン平面上の２直線 l,h が $l = h$ であるか，または交わらないとき，l と h は**平行** (parallel) であるといい，$l \parallel h$ とかく．

アフィン平面の性質

定理 11

アフィン平面において，$l_1 \parallel l_2$ かつ $l_2 \parallel l_3$ なら，$l_1 \parallel l_3$ である.

互いに平行な直線の集合で，$\mathcal{A}$ 上のどの点もそのどれかの直線上にあるような直線集合が存在する. この直線集合を（平行類 (parallel class)）という.

アフィン平面の性質

定理 12

C をアフィン平面の１つの平行類とする．そのとき C 以外の任意の直線は C のどの直線とも必ず１点で交わる．

４つの点からなる（最小の点の数）アフィン平面を $\mathrm{AG}(2,2)$ と書く．

アフィン平面の性質

系 13

アフィン平面において，平面上のすべての点を含む 2 つの直線 l, m が存在するならば，その平面は $\mathrm{AG}(2,2)$ である.

アフィン平面の性質

定理 14

もし $\mathcal{A} = (P, L, I)$ が有限アフィン平面ならば，次の性質を満たす正整数 n が存在する.

(1) 1 点を通る直線の数は $n + 1$ である.

(2) 直線上の点の数は n である.

(3) $\mathcal{A}$ の点の総数は n^2, 直線の総数は $n^2 + n$ である.

この n をアフィン平面の位数という.

射影平面

射影平面とは，次の公理を満たす結合構造 $\mathcal{P} = (P, L, I)$ である．

(P1) 任意の２点を通る直線は必ず一つ存在する．

(P2) 任意の異なる 2 直線は必ず１点で交わる．

(P3) どの３点も同一直線上にない４点が存在する．

射影平面の性質

定理 15

有限射影平面には，次のような整数 n が存在する．

(1) 各直線は必ず $n+1$ 点を通る．

(2) 任意の点は，必ず $n+1$ 直線に含まれる．

(3) $\mathcal{P}$ は n^2+n+1 個の点と n^2+n+1 個の直線を含む．

有限アフィン平面から有限射影平面の構成

$\mathcal{A} = (P, L, I)$ を有限アフィン平面とする．$\mathcal{A}$ の直線の平行類を $C_1, C_2, \ldots, C_{n+1}$ とするとき，各 C_i に含まれるすべての直線が q_i と交わるとし，$q_1, q_2, \ldots, q_{n+1}$ を通る直線を l とする．ここで新しく点集合を $P^* = P \cup \{q_1, q_2, \ldots, q_{n+1}\}$, 直線集合を $L^* = L \cup \{l\}$, 結合関係 I^* を

$$I^* = I \cup \{(q_i, m) : 1 \leq i \leq n+1, m \in C_i\} \cup \{(q_i, l) : 1 \leq i \leq n+1\}$$

とするとき，$(P*, L^*, I^*)$ は位数 n の有限射影平面となる．

$AG(2,2)$ の構成

$$
\begin{aligned}
P =& \{(x,y) : x,y \in \mathbb{F}_2\} \\
=& \{(0,0),(1,0),(0,1),(1,1)\}
\end{aligned}
$$

$$
\begin{aligned}
L = \{ & \{(0,0),(0,1)\}, && : x = 0, \\
& \{(1,0),(1,1)\}, && : x = 1, \\
& \{(0,0),(1,0)\}, && : y = 0, \\
& \{(0,1),(1,1)\}, && : y = 1, \\
& \{(0,0),(1,1)\}, && : x + y = 0, \\
& \{(0,1),(1,0)\}\} && : x + y = 1
\end{aligned}
$$

$AG(2,2)$ の点の巡回表現

$$\mathbb{F}_{2^2} = \{0, 1, \alpha, \alpha^2\},\ \alpha^2 + \alpha + 1 = 0$$

∞	0	$(0,0)$
0	1	$(1,0)$
1	α	$(0,1)$
2	α^2	$(1,1)$

$$\begin{array}{rcll}
L & = & \{\{(0,0),(0,1)\}, & : x = 0, \quad \{\infty, 1\} \\
 & & \{(1,0),(1,1)\}, & : x = 1, \quad \{0, 2\} \\
 & & \{(0,0),(1,0)\}, & : y = 0, \quad \{\infty, 0\} \\
 & & \{(0,1),(1,1)\}, & : y = 1, \quad \{1, 2\} \\
 & & \{(0,0),(1,1)\}, & : x + y = 0, \quad \{\infty, 2\} \\
 & & \{(0,1),(1,0)\}\} & : x + y = 1, \quad \{0, 1\}
\end{array}$$

$PG(2,2)$ の点の巡回表現

$$P^* = \{\infty, 0, 1, 2, q_1, q_2, q_3\}$$

$$\begin{array}{rcll}
L & = & \{\{(0,0),(0,1)\}, & : x = 0, \quad \{\infty, 1, q_1\} \\
 & & \{(1,0),(1,1)\}, & : x = 1, \quad \{0, 2, q_1\} \\
 & & \{(0,0),(1,0)\}, & : y = 0, \quad \{\infty, 0, q_2\} \\
 & & \{(0,1),(1,1)\}, & : y = 1, \quad \{1, 2, q_2\} \\
 & & \{(0,0),(1,1)\}, & : x + y = 0, \quad \{\infty, 2, q_3\} \\
 & & \{(0,1),(1,0)\}, & : x + y = 1, \quad \{0, 1, q_3\} \\
 & & \{q_1, q_2, q_3\}\}
\end{array}$$

有限射影平面の構成

有限体 $\mathbb{F}_p$ 上のベクトル空間で作られる射影平面について考えよう.
3 次元ベクトル空間の点集合は, $V = \{(x, y, z) : x, y, z \in \mathbb{F}_p\}$ で与えられる. 実数の場合と同様に V 上の同値関係を次のように定義する. $\mathbf{x} = (x, y, z), \mathbf{x}' = (x', y', z') \in V \setminus \{0\}$ に対し,

$$(x, y, z) \sim (x', y', z') \Leftrightarrow \exists \lambda \in \mathbb{F}_p \setminus \{0\} \text{ s.t. } (x, y, z) = \lambda(x', y', z')$$

このとき, 有限射影平面 $\mathbb{P}^2(\mathbb{F}_p)$ は

$$\mathbb{P}^2(\mathbb{F}_p) = \{[X : Y : 1] : (X, Y) \in \mathbb{F}_p^2\} \cup \{[x : y : 0] : (x, y) \neq (0, 0)\}$$

で与えられる.

有限射影平面の構成

また有限射影平面における直線は，V の線形独立な 2 つのベクトル $\mathbf{x}, \mathbf{y}$ が生成する 2 次元線形部分空間

$$< \mathbf{x}, \mathbf{y} >= \{\lambda\mathbf{x} + \mu\mathbf{y} : \lambda, \mu \in \mathbb{F}_p\}$$

であるので，これを射影の点集合で表すと，

$$\{\mathbf{y}\} \cup \{\mathbf{x} + \lambda\mathbf{y} : \lambda \in \mathbb{F}_p\}$$

で与えられる.

$PG(2,2)$ の点の巡回表現

$$\mathbb{F}_{2^3} = \{0, 1, \alpha, \ldots, \alpha^6\},\ \alpha^3 + \alpha + 1 = 0$$

∞	0	$(0,0,0)$
0	1	$(1,0,0)$
1	α	$(0,1,0)$
2	α^2	$(0,0,1)$
3	$\alpha^3 = 1 + \alpha$	$(1,1,0)$
4	$\alpha^4 = \alpha + \alpha^2$	$(0,1,1)$
5	$\alpha^5 = 1 + \alpha + \alpha^2$	$(1,1,1)$
6	$\alpha^6 = 1 + \alpha^2$	$(1,0,1)$

$$P^* = \{0, 1, 2, 3, 4, 5, 6\}$$

点 0 と 1 を通る直線： $\{(1,0,0), (0,1,0), (1,1,0)\}$: {0,1,3}

有限射影平面の構成

問題 6

有限射影平面 $\mathbb{P}^2(\mathbb{F}_3)$ のすべての点と直線を求めよ.

$\mathbb{P}^2(\mathbb{F}_3)$ のすべての点と直線

$\mathbb{P}^2(\mathbb{F}_3)$ の点

$$\{(0,0,1),(0,1,1),(0,2,1),(1,0,1),(1,1,1),(1,2,1),$$
$$(2,0,1),(2,1,1),(2,2,1),(0,1,0),(1,0,0),(1,1,0),(1,2,0)\}$$

$\mathbb{P}^2(\mathbb{F}_3)$ の直線
$(1,0,0)$ と $(0,1,0)$ を通る直線：

$$\{(0,1,0)\} \cup \{(1,0,0) + \lambda(0,1,0) : \lambda \in \mathbb{F}_3\}$$
$$= \{(0,1,0),(1,0,0),(1,1,0),(1,2,0)\}$$

$PG(2,3)$ の点の巡回表現

$$\mathbb{F}_{3^3} = \{0, \alpha^0 = 1, \alpha, \ldots, \alpha^{25}\},\ \alpha^3 + 2\alpha^2 + \alpha + 1 = 0$$

0	1	$(1,0,0)$	13	$\alpha^{13} = 2$	$(2,0,0)$
1	α	$(0,1,0)$	14	$\alpha^{14} = 2\alpha$	$(0,2,0)$
2	α^2	$(0,0,1)$	15	$\alpha^{15} = 2\alpha^2$	$(0,0,2)$
3	$\alpha^3 = 2 + 2\alpha + \alpha^2$	$(2,2,1)$	16	$\alpha^{16} = 2\alpha^3$	$(1,1,2)$
4	$\alpha^4 = 2 + \alpha$	$(2,1,0)$	17		$(1,2,0)$
5	$\alpha^5 = 2\alpha + \alpha^2$	$(0,2,1)$	18		$(0,1,2)$
6	$\alpha^6 = 2 + 2\alpha$	$(2,2,0)$	19		$(1,1,0)$
7	$\alpha^7 = 2\alpha + 2\alpha^2$	$(0,2,2)$	20		$(0,1,1)$
8	$\alpha^8 = 1 + \alpha + \alpha^2$	$(1,1,1)$	21		$(2,2,2)$
9	$\alpha^9 = 2 + 2\alpha^2$	$(2,0,2)$	22		$(1,0,1)$
10	$\alpha^{10} = 1 + 2\alpha^2$	$(1,0,2)$	23		$(2,0,1)$
11	$\alpha^{11} = 1 + 2\alpha + 2\alpha^2$	$(1,2,2)$	24		$(2,1,1)$
12	$\alpha^{12} = 1 + 2\alpha + \alpha^2$	$(1,2,1)$	25		$(2,1,2)$

楕円曲線

体 $\mathbb{F}$ 上で定義される楕円曲線の一般形は，次のような 3 次方程式で与えられる．これを一般ワイエルシュトラス標準形という．

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \ (a_i \in \mathbb{F}). \qquad (1)$$

$X = x/z, Y = y/z$ とすると，射影平面上の楕円曲線が次のように与えられる．

$$E : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

E と $z = 0$ との交点を無限遠点 $\mathcal{O} = [0 : 1 : 0]$ と定義する．
$E(\mathbb{F})$ でこの方程式を満たす点 $(x, y) \in \mathbb{F}^2$ と**無限遠点** $\mathcal{O} = [0 : 1 : 0]$ の集合を表す．

楕円曲線

$\mathbb{F}$ の標数が 2 でないとき，$Y' = Y + \frac{1}{2}(a_1X + a_3)$ とおけば，(1) の曲線は以下の曲線に変換できる．

$$E' : Y'^2 = X^3 + aX^2 + bX + c$$

さらに，標数が 3 でないと仮定すると，$X' = X + \frac{1}{3}a$ とおき，

$$E' : Y'^2 = X'^3 + AX' + B \tag{2}$$

となる．これを**ワイエルシュトラス標準形**という．
曲線が滑らかであるためには，X と Y に対する偏微分が同時に 0 になるような点 (特異点) を持たないことが必要である．すなわち曲線 (2) の右辺の 3 次式が重根を持たないことと同値である．
これは**判別式 $4A^3 + 27B^2$ が 0 でない**とき，かつそのときに限り成り立つ．

楕円曲線

問題 7

3 次曲線 $Y^2 = X^3 + 3X + 1$ が特異点を持つかどうか，$\mathbb{F}$ が有理数体 $\mathbb{Q}$ のとき，有限体 $\mathbb{F}_3, \mathbb{F}_5$ のときについてそれぞれ考えよ.

楕円曲線上の群

楕円曲線 (2) 上の点の足し算を定義する．楕円曲線 (2) は x 軸対称である．

定義 1

$P = (x_1, y_1), Q = (x_2, y_2)$ を楕円曲線 E' の異なる 2 点とし，$\overline{PQ}$ を P, Q を結ぶ直線とする．
直線 $\overline{PQ}$ と E との交点を R' とし（3 次曲線は射影平面上で必ず 3 点で交わるので，点 R は存在する），R' の x 軸対称の点を $R = (x_3, y_3)$ としたとき，$P + Q = R$ と定義する．

$x_1 \neq x_2$ のとき

P, Q を通る直線 $\overline{PQ}$ は, 傾きを

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

とすると

$$y = m(x - x_1) + y_1$$

であり. 楕円曲線 E' との交点は, 次の 3 次方程式の根として与えられる.

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B$$

よって, 点 R' の x 座標は

$$x = m^2 - x_1 - x_2$$

となるので, 点 $R = (x_3, y_3)$ は

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1$$

である.

$x_1 = x_2, y_1 \neq y_2$ のとき

P, Q を通る直線 $\overline{PQ}$ は, y 軸に平行な直線であるので, 楕円曲線 E' と O と交わる. よって $P + Q = O$ である.

$P = Q, y_1 \neq 0$ のとき

$P = Q$ の場合は，P を通る E' の接線 $\overline{PP}$ と E' との交点を R' とし，$\overline{RO}$ と E との交点を $R = 2P(P + P)$ とする．点 $R = (x_3, y_3)$ は

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1$$

ただし，$m = \frac{3x_1^2 + A}{2y_1}$ である．

$P = Q, y_1 = 0$ のとき

$P + Q = O$ である.

単位元

また，E' 上のすべて点 P に対して，

$$P + O = P$$

である．

可換

点 P, Q を入れ替えて考えても演算の結果は同じであることから，演算は可換である.

楕円曲線上の群

さらに，この演算により，楕円曲線の有理点の集合が群をなすことがいえる．

定理 16

楕円曲線上の点に定義した加法演算は，次の性質を満たす．

1. すべての点 $P \in E'$ に対して，$P + \mathcal{O} = P$ である．
2. 各点 $P \in E'$ に対して，$P + Q = \mathcal{O}$ となる $Q \in E'$ が存在する．Q を $-P$ と書く．
3. すべての $P, Q, R \in E'$ に対して，$(P + Q) + R = P + (Q + R)$ が成り立つ．

楕円曲線上の群

問題 8

$\mathbb{F}_5$ 上の楕円曲線 $Y^2 = X^3 + X + 1$ 上の点を列挙せよ．また，$P = (0, 1)$, $Q = (2, 1)$ に対して，$P + Q$ と $2P$ を求めよ．

楕円曲線上の離散対数問題

有限体 $\mathbb{F}_q$ 上の楕円曲線 E を考える．E 上の点 P の**位数**とは，$kP = O$ **となる最小の正整数** k である．
$< P >$ を点 P によって生成される巡回群とする．楕円曲線上の離散対数問題とは，$\forall Q \in < P >$ に対して，$kP = Q$ となる最小の k を見つけることである．
点 P の位数に非常に大きな素数が含まれるとき，k を求めるのは困難である．$a^k \equiv b(\mathrm{mod} p)$ を満たす k を求める整数上の離散対数問題に似ているが，これに比べて楕円曲線上の離散対数問題の方が計算時間がかかり，より強い強度の暗号を作ることができる．

Diffie-Hellman 鍵共有方式

アリスとボブが秘密通信をすることなく，共通鍵暗号系で用いるための鍵を共有したいとする．有限体 $\mathbb{F}_p$ 上の Diffie-Hellman 鍵共有方式は，以下の通りである．

1. p を大きな素数とし，α を乗法群 $\mathbb{F}_p^*$ の生成元とする．この p と g は公開されているものとする．
2. アリスは秘密鍵 a を選び，$A = \alpha^a (\mathrm{mod} p)$ を公開する．
3. ボブは秘密鍵 b を選び，$B = \alpha^b (\mathrm{mod} p)$ を公開する．
4. アリスは秘密鍵 a とボブの公開鍵 B を用いて，$B^a = \alpha^{ab}$ を計算する．
5. ボブは秘密鍵 b とアリスの公開鍵 A を用いて，$A^b = \alpha^{ab}$ を計算する．
6. アリスとボブは鍵 α^{ab} を共有する．

Diffie-Hellman 鍵共有方式:楕円曲線版

これを楕円曲線上に拡張した鍵共有方式は，以下の通りである.

1. 有限体 $\mathbb{F}_q$ 上の楕円曲線 E と，E 上の点 P を公開する. ただし P の位数は大きいものとする.
2. アリスは秘密鍵 a を選び，$P_a = aP$ を公開する.
3. ボブは秘密鍵 b を選び，$P_b = bP$ を公開する.
4. アリスは秘密鍵 a とボブの公開鍵 P_b を用いて，$aP_b = abP$ を計算する.
5. ボブは秘密鍵 b とアリスの公開鍵 P_a を用いて，$bP_a = abP$ を計算する.
6. アリスとボブは鍵 abP を共有する.

Diffie-Hellman 問題

盗聴者イブは，E, P, P_a, P_b から次の問題を解くことが必要となる．

Diffie-Hellman 問題 楕円曲線 E 上の点 P, aP, bP が与えられたとき，abP を求めよ．

Decision Diffie-Hellman 問題 楕円曲線 E 上の点 P, aP, bP と Q が与えられたとき，$Q = abP$ であるか判定せよ．

ElGamal 暗号

公開鍵暗号方式の一つである有限体 $\mathbb{F}_p$ 上の ElGamal 暗号は，以下の通りである．

1. アリスがボブにメッセージを送信したいものとする．受信者ボブは大きな素数 p，乗法群 $\mathbb{F}_p^*$ の生成元 α を選ぶ．次にボブは秘密鍵 b を選び，$B = \alpha^b \pmod{p}$ を計算し，(p, α, B) を公開する．
2. 送信者アリスは，ボブの公開鍵 (p, α, B) と送信したいメッセージ $m \in \mathbb{F}_p^*$ と乱数 r から暗号文 (c_1, c_2) を次のように計算し，ボブに送る．

$$c_1 = \alpha^r \pmod{p},$$

$$c_2 = mB^r \pmod{p}$$

3. ボブは秘密鍵 b を用いて，$c_2/c_1^b \pmod{\mathrm{p}}$ を計算し，メッセージ m を得る．

ElGamal 暗号: 楕円曲線版

これを楕円曲線上に拡張した ElGamal 暗号方式は，以下の通りである．

1. アリスがボブにメッセージを送信したいものとする．受信者ボブは有限体 $\mathbb{F}_q$ 上の楕円曲線 E と，E 上の点 P を選ぶ．ただし P の位数は大きいものとする．次にボブは秘密鍵 b を選び，$B = bP$ を計算し，(E, P, B) を公開する．
2. 送信者アリスは，ボブの公開鍵 (E, P, B) と送信したいメッセージ $m \in E$ と乱数 r から暗号文 (c_1, c_2) を次のように計算し，ボブに送る．

$$c_1 = rP,$$

$$c_2 = m + rB$$

3. ボブは秘密鍵 b を用いて，$c_2 - bc_1$ を計算し，メッセージ m を得る．

ElGamal 暗号: 楕円曲線版

例 1

$\mathbb{F}_{17}$ 上の楕円曲線 $E : Y^2 = X^3 + X + 3$ 上の点は，無限遠点 O と

$$(2, \pm 8), (3, \pm 4), (6, \pm 2), (7, \pm 8), (8, \pm 8), (11, \pm 6), (12, \pm 3), (16, \pm 1)$$

の 17 点である. 演算表は表 1 の通りである.

ElGamal 暗号: 楕円曲線版

例 2

上記の楕円曲線 E において，点 $P = (2, 8)$ とし，Diffie-Hellman 鍵共有方式を考える. アリスとボブの秘密鍵をそれぞれ $a = 5, b = 6$ とする. このとき，アリスとボブの公開鍵は

$$P_a = aP = (7, 9),$$

$$P_b = bP = (6, 15)$$

であり，共有鍵は $abP = (8, 9)$ である.

ElGamal 暗号: 楕円曲線版

例 3

同様に，上記の楕円曲線 E において，ElGamal 暗号方式を考える. 受信者ボブは点 $P = (2, 8)$ と秘密鍵 $b = 6$ を選び，$B = bP = (6, 15)$ を求め，(E, P, B) を公開する. アリスの送信したいメッセージを $m = (8, 8)$，乱数 $r = 3$ とすると，暗号文 (c_1, c_2) は

$$c_1 = 3P = (16, 16)$$

$$c_2 = m + rB = (8, 8) + (2, 8) = (7, 9)$$

となる. ボブは秘密鍵 $b = 6$ を用いて，

$$c_2 - bc_1 = (7, 9) - (2, 8) = (7, 9) + (2, 9) = (8, 8)$$

を得る.

離散対数問題への攻撃法

楕円曲線上の離散対数問題（Diffie-Hellman 問題）への攻撃法として，Baby-Step-Giant-Step 法, Pollard の ρ 法, λ 法がある．これらは群 G の位数を n とすれば, n の平方根 $O(\sqrt{n})$ オーダーの攻撃法として知られている.
$P, Q \in G$ が与えられたとき, $Q = lP$ となる整数 l を求めたい.

Baby-Step-Giant-Step 法

Baby-Step-Giant-Step 法

1. $m \geq \sqrt{n}$ となる整数 m を選び, mP を計算する.
2. $0 \leq i < m$ に対して, iP をストックしておく.
3. $Q - jmP,\ j = 0, 1, \ldots, m-1$ を計算し, ストックしてある iP と一致するまで繰り返す.
4. $iP = Q - jmP$ であれば, $Q = lP,\ l \equiv i + jm \pmod{n}$ である.

Polland の ρ 法

ρ 法

与えられた点 Q に対して，$Q = lP$ となる整数 l を求める.

1. G の元をほぼ均等に S_1, S_2, S_3 に分け，関数 F を

$$F(R) = \begin{cases} R + Q & R \in S_1 \text{のとき} \\ 2R & R \in S_2 \text{のとき} \\ R + P & R \in S_3 \text{のとき} \end{cases}$$

と定義する.

ρ 法

ρ 法続き

2. 任意の点 $R_0 = a_0P + b_0Q$ から始め，$R_{i+1} = F(R_i)$ により，G の元の列 $\{R_i\}, i = 0, 1, \ldots$ を定義する.
3. $R_i = a_iP + b_iQ$ とする.
4. $R_j = R_k$ となったとする．このとき，
   $a_jP + b_jQ = a_kP + b_kQ$ であり，

$$(b_k - b_j)Q = (a_j - a_k)P$$

   が成り立つ.
5. $\gcd(b_k - b_j, n) = 1$ ならば，$l = (a_j - a_k)(b_k - b_j)^{-1} \pmod{n}$ と求まる.

ρ 法の例

例 4

例 1 の楕円曲線 E を考える.
$P = (2, 8)$, $Q = (8, 9)$ とし，$Q = lP$ となる l を求める.
$S_1 = \{(2, \pm 8), (3, \pm 4), (6, \pm 2)\}$, $S_2 = \{(7, \pm 8), (8, \pm 8), (11, \pm 6)\}$,
$S_3 = \{(12, \pm 3), (16, \pm 1), O\}$ とする.

1. $R_0 = P + Q$ を求めると，$(16, 1) \in S_3$ より,
   $R_1 = F(R_0) = R_0 + P = 2P + Q = (12, 14)$ となる.
2. $R_1 \in S_3$ より，$R_2 = F(R_1) = R_1 + P = 3P + Q = (2, 9)$ となる.
3. $R_2 \in S_1$ より，$R_3 = F(R_2) = R_2 + Q = 3P + 2Q = (7, 8)$ となる.
4. $R_3 \in S_2$ より，$R_4 = F(R_3) = 2R_3 = 6P + 4Q = (11, 6)$ となる,

ρ 法の例

例 4 続き

5. $R_4 \in S_2$ より，$R_5 = F(R_4) = 2R_4 = 12P + 8Q = (16, 1)$ となる.
6. ここで，$R_5 = R_0$ となったので，$P + Q = 12P + 8Q$. すなわち，$7Q = -11P = 6P$ である.
7. すなわち $l = 6 \cdot 7^{-1} = 6 \cdot 5 = 30 = 13$，$Q = 13P$ を得る.

λ法（カンガルー法)

ρ法と同様に与えられた点Qに対して，$Q = lP$となる整数lを求める．lの値が比較的小さいときに有効とされている．

λ法

ある規定された範囲の整数を値域Vに持つ関数$g : G \to V$を定め，Fを

$$F(R) = R + g(R)P$$

と定義する，$l < a_0$と仮定する．

1. 飼いならしたカンガルーのジャンプ：
   $R_0 = a_o P$とし，$R_{i+1} = F(R_i)$により点列$\{R_i\}$を生成する．$R_i = a_i P$とする．
   これを適当な回数（k回）行い，トータルのジャンプ距離$\sum_{i=0}^{k-1} g(R_i)$を記録し，最後の着地点R_sに穴を掘る．

λ法（カンガルー法)

λ法続き

2. 野生のカンガルーのジャンプ：
   $T_0 = Q$ とし，$T_{i+1} = F(T_i)$ により点列生成をし，トータルのジャンプ距離 $\sum_{i=0} g(T_i)$ が $a_0 + \sum_{i=0}^{k-1} g(R_i)$ を超えるまで行い，R_s に落ちるか監視する．$T_i = Q + b_i P$ とする．
3. $R_s = T_t$ となったとする．このとき，$a_s P = Q + b_t P$ であり，
   $$Q = (a_s - b_t)P$$
   が成り立つ．
4. 野生のカンガルーが R_s に落ちなかった場合には，比較的小さな b_0 に対し，$T_0 = Q + b_0 P$ と取り直す．
5. 野生のカンガルーが飼いならしたカンガルーのどこかの着地点に降りたとすると，その後の軌跡は全く同じものとなる．

λ 法の例

例 5

例 1 の楕円曲線 E を考える． $P = (2, 8)$, $Q = (11, 6)$, $l < 8 (= a_0)$ **と仮定** $V = \{1, 2, 3, 4\}$ **とし，** g **を**

G	$\to$	V
$\mathcal{O}$, $(2, \pm 8)$, $(3, \pm 4)$		1
$(6, \pm 2)$, $(7, \pm 8)$		2
$(8, \pm 8)$, $(11, \pm 6)$		3
$(12, \pm 3)$, $(16, \pm 1)$		4

とする.

λ法の例

例 5 続き

$k = 3$ とする.

1. $R_0 = a_0 P = 8P$ を求めると, $(3, 13)$ より,
   $R_1 = F(R_0) = R_0 + g(R_0)P = R_0 + P = 9P = (3, 4)$ となる.
2. $R_2 = F(R_1) = R_1 + g(R_1)P = R_1 + P = 10P = (11, 11)$ となる.
3. $R_3 = F(R_2) = R_2 + g(R_2)P = R_2 + 3P = 13P = (8, 9)$ となる.
4. 飼いならしたカンガルーのジャンプ距離 $\sum_{i=0}^{2} g(R_i) = 5$ である.

λ法の例

例 5 続き

6. $T_0 = Q$ より,
   $T_1 = F(T_0) = T_0 + g(T_0)P = T_0 + 3P = Q + 3P = (11, 11)$
   となる.
7. $T_1 = (11, 11)$ より,
   $T_2 = F(T_1) = T_1 + g(T_1)P = T_1 + 3P = Q + 6P = (8, 9)$ となる.
8. $R_3 = T_2$ となったので, $13P = Q + 6P$ であり,

$$Q = 7P$$

   を得る.