1　行列式と幾何

初めに，2次および3次の正方行列の行列式の性質を思い出し，それらが表現するものを確認しよう．

2次の正方行列 $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ の行列式を $\det A=\det(\mathbf{u},\mathbf{v})$ と表す．ただし $\mathbf{u}=\begin{pmatrix} a \\ c \end{pmatrix}$, $\mathbf{v}=\begin{pmatrix} b \\ d \end{pmatrix}$ とする．

定理 1 行列式 $detA=det(\mathbf{u},\mathbf{v})$ は次の性質を満たす．

1. 単位行列 $E=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ に対して，$detE=1$ である．
2. α,β を定数として
$$det(\alpha\mathbf{u}+\beta\mathbf{u}',\mathbf{v})=\alpha det(\mathbf{u},\mathbf{v})+\beta det(\mathbf{u}',\mathbf{v})$$
3. $det(\mathbf{u},\mathbf{v})=-det(\mathbf{v},\mathbf{u})$
4. $det(\mathbf{u},\mathbf{u})=0$

定理 2 *2*つのベクトル $\mathbf{u}$, $\mathbf{v}$ によって張られる平行四辺形の面積は，$|det(\mathbf{u},\mathbf{v})|$ で表される．

問題 1 定理 *2* を示せ．

3次の正方行列 $A=\begin{pmatrix} u_1 & v_1 & w_1 \\ u_2 & v_2 & w_2 \\ u_3 & v_3 & w_3 \end{pmatrix}$ の行列式を $\det A=\det(\mathbf{u},\mathbf{v},\mathbf{w})$ と表す．ただし $\mathbf{u}=\begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix}$, $\mathbf{v}=\begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}$, $\mathbf{w}=\begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix}$ とする．

定理 3 行列式 $detA=det(\mathbf{u},\mathbf{v},\mathbf{w})$ は次の性質を満たす．

1. 単位行列 $E=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ に対して，$detE=1$ である．
2. α,β を定数として
$$det(\alpha\mathbf{u}+\beta\mathbf{u}',\mathbf{v},\mathbf{w})=\alpha det(\mathbf{u},\mathbf{v},\mathbf{w})+\beta det(\mathbf{u}',\mathbf{v},\mathbf{w})$$
3. 任意の *2*列を入れ替えると，行列式は符号を変える．$det(\mathbf{u},\mathbf{v},\mathbf{w})=-det(\mathbf{v},\mathbf{u},\mathbf{w})=det(\mathbf{v},\mathbf{w},\mathbf{u})$
4. 同一のベクトルを *2*列以上含む行列の行列式は，*0*である．$det(\mathbf{u},\mathbf{u},\mathbf{w})=det(\mathbf{u},\mathbf{v},\mathbf{v}))=0$

$$\begin{aligned}\det A &= \begin{vmatrix} u_1 & v_1 & w_1 \\ u_2 & v_2 & w_2 \\ u_3 & v_3 & w_3 \end{vmatrix} \\ &= u_1v_2w_3 + u_2v_3w_1 + u_3v_1w_2 - u_1v_3w_2 - u_2v_1w_3 - u_3v_2w_1 \\ &= \begin{vmatrix} v_2 & w_2 \\ v_3 & w_3 \end{vmatrix} u_1 + \begin{vmatrix} v_3 & w_3 \\ v_1 & w_1 \end{vmatrix} u_2 + \begin{vmatrix} v_1 & w_1 \\ v_2 & w_2 \end{vmatrix} u_3\end{aligned}$$

である. このとき $\mathbf{v}$ と $\mathbf{w}$ の外積を

$$\mathbf{v} \times \mathbf{w} = \left(\begin{vmatrix} v_2 & w_2 \\ v_3 & w_3 \end{vmatrix}, \begin{vmatrix} v_3 & w_3 \\ v_1 & w_1 \end{vmatrix}, \begin{vmatrix} v_1 & w_1 \\ v_2 & w_2 \end{vmatrix} \right)$$

とすると,

$$\det A = \mathbf{u} \cdot (\mathbf{v} \times \mathbf{w})$$

と書ける.

定理 4 *3*つのベクトル $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w}$ によって張られる平行六面体の体積は，$|det(\mathbf{u}, \mathbf{v}, \mathbf{w})|$ で表される.

定理 5 *2*つのベクトル $\mathbf{u}$, $\mathbf{v}$ の外積 $\mathbf{u} \times \mathbf{v}$ は $\mathbf{u}$, $\mathbf{v}$ に直交しており, その長さは $\mathbf{u}$, $\mathbf{v}$ を *2*辺とする平行四辺形の面積に等しい.

次に xy 座標平面上の直線の方程式を行列式を用いて表してみよう．直線の方程式の一般形は

$$ax + by = c \quad (a \neq 0 \text{ または } b \neq 0)$$

で表されるが，直線の方向と直線の通る 1 点を与えて定めるパラメータ表現がある．直線の方向を $\mathbf{v} = \begin{pmatrix} \xi \\ \eta \end{pmatrix}$ として，点 $\mathbf{p} = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$ を通るとするとき，直線上の点はパラメータ t を用いて

$$\mathbf{x}(t) = t\mathbf{v} + \mathbf{p} \quad (t \in \mathbb{R})$$

と表すことができる．さらに行列式を用いて

$$\det(\mathbf{v}, \mathbf{x}) = \det(\mathbf{v}, \mathbf{p})$$

とも表すことができる．また，2 点 $\mathbf{p} = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$, $\mathbf{q} = \begin{pmatrix} \gamma' \\ \delta' \end{pmatrix}$ を通る直線の方程式は

$$\det(\mathbf{x}, \mathbf{q}) + \det(\mathbf{p}, \mathbf{x}) = \det(\mathbf{p}, \mathbf{q})$$

と表すことができる.

問題 2 (1) 法線方向が $\mathbf{n} = (a, b)^{\mathsf{T}}$ で, 点 $\mathbf{p} = (\gamma, \delta)^{\mathsf{T}}$ を通る直線の方程式が

$$\mathbf{n} \cdot \mathbf{x} = \mathbf{n} \cdot \mathbf{p}, \quad ax + by = c, \text{ただし, } c = a\gamma + b\delta \text{ とする.}$$

で与えられることを示せ.

(2) 方向が $\mathbf{v} = (\xi, \eta)^\mathsf{T}$ で, 点 $\mathbf{p} = (\gamma, \delta)^\mathsf{T}$ を通る直線の方程式が

$$\mathbf{x} = t\mathbf{v} + \mathbf{p}, \quad det(\mathbf{v}, \mathbf{x}) = det(\mathbf{v}, \mathbf{p})$$

で与えられることを示せ.

(3) *2* 点 $\mathbf{p} = (\gamma, \delta)^\mathsf{T}$, $\mathbf{q} = (\gamma', \delta')^\mathsf{T}$ を通る直線の方程式が

$$det(\mathbf{x}, \mathbf{q}) + det(\mathbf{p}, \mathbf{x}) = det(\mathbf{p}, \mathbf{q})$$

で与えられることを示せ.

最後に 3 点を通る平面の方程式を行列式を用いて与えてみよう．まず平面は二次元なので 2 つの独立なベクトル $\mathbf{u}$, $\mathbf{v}$ を用いて，$s\mathbf{u} + t\mathbf{v}$ は $\mathbf{u}$, $\mathbf{v}$ を 2 辺とする平行四辺形を含む原点を通る平面上の点を表している．そこで空間内の一点 $\mathbf{p}$ を与えると，点 $\mathbf{p}$ を通り方向が $\mathbf{u}$, $\mathbf{v}$ の平面上の任意の点は,

$$\mathbf{x} = s\mathbf{u} + t\mathbf{v} + \mathbf{p}$$

としてパラメータ表現することができる.

三角形の頂点をなす 3 点 $\mathbf{p}$, $\mathbf{q}$, $\mathbf{r}$ を通る平面 H は，平面を定める 2 つのベクトルを $\mathbf{u} = \mathbf{p} - \mathbf{r}$, $\mathbf{v} = \mathbf{q} - \mathbf{r}$ と考えることで

$$\det(\mathbf{p} - \mathbf{r}, \mathbf{q} - \mathbf{r}, \mathbf{x} - \mathbf{r}) = 0 \tag{1}$$

で与えられる.

問題 3 平面 H が *(1)* で与えられることを示せ.

2　ユークリッド幾何

幾何学の始まりは，紀元前 3 世紀に遡る．古代ギリシャの数学者ユークリッド（ギリシャ語ではエウクレイデス）は，平面幾何，比例理論，数論，無理数論，立体幾何などをその著書「ユークリッド原論」全 13 巻に定義，公準•公理，命題の形式でまとめた．定義とは，ものごとの意味を定めるもの，公理とは，議論の前提として導入する仮定のこと，命題とは，公理に基づいて示される性質である．原論では数学全体に関する公理を「公理」，幾何に関する公理を「公準」と呼んでいる．

ユークリッド原論の第 1 巻の定義は以下のようなものである (ユークリッド原論追補版，共立出版より引用)．

1. 点とは部分をもたないものである．
2. 線とは幅のない長さである．
3. 線の端は点である．
4. 直線とはその上にある点について一様に横たわる線である．
5. 面とは長さと幅のみをもつものである．
6. 平面とはその上にある直線について一様に横たわる面である．
7. 平面角とは平面上にあって互いに交わりかつ一直線をなすことのない二つの線相互のかたむきである．
8. 角をはさむ線が直線であるとき，その角は直線角とよばれる．
9. 直線が直線の上に立てられて接角を互いに等しくするとき，等しい角の双方は直角であり，上に立つ直線はその下の直線に対して垂線とよばれる．
10. 鈍角とは直角より大きい角である．
11. 鋭角とは直角より小さい角である．
12. 境界とはあるものの端である．
13. 図形とは一つあたは二つ以上の境界によってかこまれたものである．
14. 円とは一つの線にかこまれた平面図形で，その図形の内部にある 1 点からそこへひかれたすべての線分が互いに等しいものである．
15. この点は円の中心とよばれる．
16. 円の直径とは円の中心を通り両方向で円周によって限られた任意の線分であり，それはまた円を 2 等分する．
17. 半円とは直径とそれによって切り取られた弧とによってかこまれた図形である．半円の中心は円のそれと同じである．

18. 直線図形とは線分にかこまれた図形であり，三辺形とは三つの，四辺形とは四つの，多辺形とは四つより多くの線分にかこまれた図形である．

19. 三辺形のうち，等辺三角形と三つの等しい辺をもつもの，二等辺三角形とは二つだけ等しい辺をもつもの，不等辺三角形とは三つの不等な辺をもつものである．

20. さらに三辺形のうち，直角三角形とは直角をもつもの，鈍角三角形とは鈍角をもつもの，鋭角三角形とは三つの鋭角をもつものである．

21. 四辺形のうち，正方形とは等辺でかく角が直角のもの，矩形とは角が直角で，等辺でないもの，菱形とは等辺で，角が直角でないもの，直斜方形とは対辺と対角が等しいが，等辺でなく角が直角でないものである．　これら以外の四辺形はトラペジオンとよばれるとせよ．

22. 平行線とは，同一の平面上にあって，両方向に限りなく延長しても，いずれの方向においても互いに交わらない直線である．

次に公準の部分を紹介する．次のことが要請されているとせよ．

1. 任意の点から任意の点へ直線をひくこと．

2. および有限直線を連続して一直線に延長すること．

3. および任意の点と距離（半径）とをもって円を描くこと．

4. およびすべての直角は互いに等しいこと．

5. および 1 直線が 2 直線に交わり同じ側の内角の和を 2 直角より小さくするならば，この 2 直線は限りなく延長されると 2 直角より小さい角のある側において交わること．

上の 5 が「平行線の公理」と呼ばれるもので，近代では

5' 直線外の一点を通ってその直線に平行な直線は一本あって一本に限る．

として理解されている．　これら 1 から 5 の公準に基づいた幾何学を**ユークリッド幾何学**，平行線の公理を仮定しない幾何学を**非ユークリッド幾何学**という．

第 1 巻に記されている 48 個の命題は中学•高校で学んだなじみ深い幾何の性質を扱ったものである．

命題 1 与えられた有限な直線（線分）の上に正三角形をつくること (正三角形の作図)．

命題 2 与えられた点において与えられた線分に等しい線分をつくること．

命題 3 不等な 2 線分が与えられ, 大きいほうから小さいほうに等しい線分を切り取ること．

命題 4 2 辺と狭角の等しい二つの三角形は相等しい (三角形の合同条件)．

命題 5 二等辺三角形の定角は相等しい．底辺の下側の角も相等しい．

命題 6 5 の逆．

命題 7 同一底辺上に同じ側に等しい辺を持つ二つの三角形はつくられない (三角形の作図の一意性)．

命題 8 3 辺のそれぞれ等しい二つの三角形は相等しい (三角形の合同条件).

命題 9 与えられた角を 2 等分すること.

命題 10 与えられた線分を 2 等分すること.

命題 11 与えられた直線に，その上の与えられた点から直角に直線をひくこと.

命題 12 与えられた無限直線にその上にない与えられた点から垂線を下すこと.

命題 13 一直線上の二つの接角の和は２直角に等しい.

命題 14 13 の逆.

命題 15 対頂角は等しい.

命題 16 三角形の外角は内対角の一つより大きい.

命題 17 三角形の２角の和は２直角より小さい.

命題 18 三角形の大きい辺は大きい角に対する.

命題 19 18 の逆.

命題 20 三角形の２辺の和は第３辺より大きい.

命題 21 三角形の内部に同一底辺上に立つ三角形がつくられれば，後者の残りの２辺の和は前者の残りの２辺の和より小さいが，より大きい角をはさむ.

命題 22 与えられた３線分から三角形をつくること.

命題 23 与えられた線分上にその上の点において与えられた角に等しい角をつくること.

命題 24 ２辺をそれぞれ等しくする二つの三角形のうち，等しい辺にはさまれる角が大きい方が大きい対辺をもつ.

命題 25 24 の逆

命題 26 ２角と 1 辺を等しくする二つの三角形は相等しい (三角形の合同条件).

命題 27 錯角が等しければ２直線は平行である.

命題 28 外角が同側の内対角に等しいかまたは同側内角の和が 2 直角に等しければ，２直線は平行である.

命題 29 27, 28 の逆

命題 30 同じ直線に平行な２直線は互いに平行である.

命題 31 与えられた点を通り与えられた直線に平行線をひくこと.

命題 32 三角形の外角は二つの内対角の和に等しく，内角の和は 2 直角である.

命題 33 等しく平行な 2 線分を同じ側で結ぶ 2 線分も等しく平行である.

命題 34 平行四辺形の対角線はこれを 2 等分し，対辺，対角は等しい.

命題 35 同底で同じ平行線の間にある平行四辺形は相等しい.

命題 36 等底で同じ平行線の間にある平行四辺形は相等しい.

命題 37 同底で同じ平行線の間にある三角形は相等しい.

命題 38 等底で同じ平行線の間にある三角形は相等しい.

命題 39 37 の逆

命題 40 38 の逆

命題 41 同底で同じ平行線の間にある平行四辺形は三角形の 2 倍である.

命題 42 与えられた直線角のなかに与えられた三角形に等しい平行四辺形をつくること.

命題 43 平行四辺形の対角線をはさむ二つの補形は等しい.

命題 44 与えられた線分上に与えられた直線角のなかに与えられた三角形に等しい平行四辺形をつくること.

命題 45 与えらえた直線角のなかに与えられた直線図形に等しい平行四辺形をつくること.

命題 46 与えられた線分上に正方形を描くこと.

命題 47 直角三角形の斜辺の上の正方形は他の 2 辺の上の正方形の和に等しい (ピタゴラスの定理).

命題 48 47 の逆.

3　黄金比と正五角形

線分 AB を二つにわけ，$AB = AC + BC$ $(AC > BC)$ とする．全体 AB が大きい部分 AC に対するように，大きい部分 AC が小さい部分 BC に対するとき，黄金比に分けられたという．「与えられた線分を黄金比 (外中比) に分けること」としてユークリッド原論第 6 巻命題 30 に黄金比に関しての作図法も示されている．黄金比を求めると，$AC : BC = \frac{1+\sqrt{5}}{2} : 1$ であることがわかる．

問題 4 黄金比を持つ長方形を作図せよ．

問題 5 線分を黄金比に分けよ．

中心 O の円 O が与えられているとき、円 O に内接する正五角形を次の手順で作図する．

1. 点 O を通る任意の直線を引き円 O との交点を A, B とする
2. 線分 AB の垂直二等分線を引き，円 O との交点を C とする．
3. 線分 OC の中点を D とする．
4. 中心 D, 半径 AD の円を描き，直線 OC との交点を E とする．
5. 中心を A, 半径 OE の円を描き，円 O との交点を F, G とする．
6. 中心を B, 半径 FG の円を描き，円 O との交点を H,I とする．
7. 点 B, H, G, F, I を順に結べば正五角形 $BHGFI$ が得られる．

問題 6 正五角形の対角線の長さと 1 辺の比が黄金比となることを示せ．

4　射影幾何学

4.1　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．

問題 7 点 B が $(x - pz/r, y - qz/r, 0)$ として与えられることを示せ．

4.2　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 8 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．

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 6 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．

この定理を次のような例を用いて見ていこう．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．

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

定理 7 平面上の平行な 2 直線は無限遠点で交わる.

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.

次に射影幾何学において重要な定理のいくつかを紹介する.

定理 8 (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.

定理 9 (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.

定理 10 (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.

4.3 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．

代数的に表現すると，$\mathbf{x} = (x,y,z)$, $\mathbf{x}' = (x',y',z') \in \mathbb{R}^3 \setminus \{0\}$ 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．(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．

定理 11 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

4.4 射影平面を公理から

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

定理 12 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．

定理 13 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 AG$(2,2)$ と書く．

系 14 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 $AG(2,2)$ である．

定理 15 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．

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

(A1) 任意の 2 点を通る直線は必ず一つ存在する．

(A2) 任意の異なる 2 直線は必ず 1 点で交わる．

(A3) どの 3 点も同一直線上にない 4 点が存在する．

定理 16 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．

次に，有限アフィン平面から有限射影平面を構成してみよう．$\mathcal{A} = (P, L, I)$ 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

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

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

4.5　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．

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．

問題 9 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．

5　楕円曲線暗号

5.1　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．

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

$X = x/z$,$Y = y/z$ 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．

$\mathbb{F}$ の標数が 2 でないとき，$Y' = Y + \frac{1}{2}(a_1X + a_3)$ とおけば, (2) 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，

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

となる．これをワイエルシュトラス標準形をいう．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 (3) 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．

問題 10 *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．

5.2　楕円曲線上の群

楕円曲線 (3) 上の点の足し算を定義する．楕円曲線 (3) 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 $\mathcal{O}$ と交わる． よって $P + Q = \mathcal{O}$ 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 $P + Q = \mathcal{O}$ である．

また，E' 上のすべて点 P に対して，

$$P + \mathcal{O} = P$$

である．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．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 17 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．

問題 11 $\mathbb{F}_5$ 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．

5.3 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，$kP = \mathcal{O}$ 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．

5.4 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．

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．

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 上の与えられた P, aP, bP と Q が与えられたとき，$Q = abP$ であるか判定せよ．

5.5 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，$B = \alpha^b (\mathrm{mod}\ p)$ 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．

$$c_1 = \alpha^r (\mathrm{mod}\ p),$$

$$c_2 = mB^r (\mathrm{mod}\ p)$$

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

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．

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 $\mathcal{O}$ 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．

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．

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．

	(2,8)	(2,9)	(3,4)	(3,13)	(6,2)	(6,15)	(7,8)	(7,9)	(8,8)	(8,9)	(11,6)	(11,11)	(12,3)	(12,14)	(16,1)	(16,16)
(2,8)	(12,3)	$\mathcal{O}$	(11,11)	(3,4)	(7,8)	(11,6)	(8,9)	(6,15)	(7,9)	(16,1)	(3,13)	(6,2)	(16,16)	(2,9)	(12,14)	(8,8)
(2,9)	$\mathcal{O}$	(12,14)	(3,13)	(11,6)	(11,11)	(7,9)	(6,2)	(8,8)	(16,16)	(7,8)	(6,15)	(3,4)	(2,8)	(16,1)	(8,9)	(12,3)
(3,4)			(2,8)	$\mathcal{O}$	(16,16)	(12,14)	(8,8)	(16,1)	(8,9)	(7,9)	(2,9)	(12,3)	(6,2)	(11,6)	(6,15)	(7,8)
(3,13)				(2,9)	(12,3)	(16,1)	(16,16)	(8,9)	(7,8)	(8,8)	(12,14)	(2,8)	(11,11)	(6,15)	(7,9)	(6,2)
(6,2)					(7,9)	$\mathcal{O}$	(6,15)	(2,9)	(12,14)	(11,6)	(2,8)	(8,8)	(8,9)	(3,4)	(3,13)	(16,1)
(6,15)						(7,8)	(2,8)	(6,2)	(11,11)	(12,3)	(8,9)	(2,9)	(3,13)	(8,8)	(16,16)	(3,4)
(7,8)							(11,6)	$\mathcal{O}$	(2,9)	(3,13)	(12,3)	(7,9)	(16,1)	(11,11)	(3,4)	(12,14)
(7,9)								(11,11)	(3,4)	(2,8)	(7,8)	(12,14)	(11,6)	(16,16)	(12,3)	(3,13)
(8,8)									(3,13)	$\mathcal{O}$	(6,2)	(16,1)	(6,15)	(12,3)	(2,8)	(11,6)
(8,9)										(3,4)	(16,16)	(6,15)	(12,14)	(6,2)	(11,11)	(2,9)
(11,6)											(16,1)	$\mathcal{O}$	(3,4)	(7,9)	(8,8)	(11,11)
(11,11)												(16,16)	(7,8)	(3,13)	(11,6)	(8,9)
(12,3)													(8,8)	$\mathcal{O}$	(2,9)	(7,9)
(12,14)														(8,9)	(7,8)	(2,8)
(16,1)															(6,2)	$\mathcal{O}$
(16,16)																(6,15)

表 1: 演算表

$P = (2,8)$ とすると，P の位数は 17 である.

$2P$	$3P$	$4P$	$5P$	$6P$	$7P$	$8P$	$9P$	$10P$	$11P$	$12P$	$13P$	$14P$	$15P$	$16P$	$17P$
(12,3)	(16,16)	(8,8)	(7,9)	(6,15)	(11,6)	(3,13)	(3,4)	(11,11)	(6,2)	(7,8)	(8,9)	(16,1)	(12,14)	(2,9)	$\mathcal{O}$