2021 年度相原学部ゼミコメント *

(2021 年 12 月 23 日更新)

これは, 2021 年度相原学部ゼミでの不足を補うためのノートである[*1].

目次

1 平行六面体

この節では, 教科書 [CVL, Theorem 1.26] で使われている「平行六面体」について述べる. 3 次元平行六面体は学部の線型数学でも扱われることがあるが, より一般の n 次元平行六面体については (少なくても本学の) 線型数学の範疇を超えるので, ここで言及した

* 教科書は [CVL]

[*1] ただし, ゼミの内容のすべてをフォローしているわけではない.

い[*2]. (本学の線型数学の知識は既知とする. また, 幾何学 I, II の講義内容と被る箇所が多々あると思うが, 参考のため記す.)

以下, K を $\mathbb{R}$ または $\mathbb{C}$ とし, V を K 上の n 次元ベクトル空間とする. また, 複素数 α に対して, $\overline{\alpha}$ で α の複素共役を表す.

$K = \mathbb{R}$ とする. V 内における**平行六面体**とは, ベクトル $v_1, \cdots, v_m$ で作られる立体

$$P = \{\alpha_1 v_1 + \cdots + \alpha_m v_m \mid 0 \leq \alpha_i \leq 1,\ i = 1, \cdots, m\}$$

である. この節の目標は, P の体積を定義し, それを求めることである. (線型数学の延長として書くため, できるだけ $K = \mathbb{R}$ を仮定しない. ただし, 内積を考える必要があるため, $K = \mathbb{R}$ or $\mathbb{C}$ とした.)

1.1 内積

まずは, 長さおよび直交性の概念を作る内積を定義する.

定義 1.1. 次を満たす写像 $(-, ?) : V \times V \to K$ を考える: $u, v, w \in V, \alpha \in K$,

(1) $(u, v) = \overline{(v, u)}$;
(2) $(u + v, w) = (u, w) + (v, w)$;
(3) $(\alpha u, v) = \alpha(u, v)$;
(4) $(u, u) \geq 0$, ただし等号成立は $u = 0$ に限る.

このような写像をもつベクトル空間 V を**計量ベクトル空間**といい, (u, v) を u, v の**内積**という.

定義からすぐにわかるように, 次が成り立つ:
① $(u, 0) = (0, u) = 0$; ② $(u, v + w) = (u, v) + (u, w)$; ③ $(u, \alpha v) = \overline{\alpha}(u, v)$.
(① において, 数の " 0 " とベクトルの " 0 " を同じ記号を用いて書いたが, 注意!)

高校数学でも学ぶように, 次が典型的な内積の例である.

例 1.2. $V = K^n$ (n 次元数ベクトル空間) とする. ただし, ベクトル u は縦ベクトルで考え, 行列として見たときの転置を ${}^t u$ と表す. また, 成分すべてに複素共役を適用したベクトルを $\overline{u}$ とする. このとき, $u, v \in V$ に対して,

$$(u, v) = {}^t u \cdot \overline{v} \text{ (通常の行列の積)}$$

[*2] ゼミ本題の【デザイン論】から離れ過ぎないようになるべく最短で学べるよう, 背景は後回しにして必要な部分から書いていこうと思う.

と定義すると, これは内積の公理を満たし, V は計量ベクトル空間となる. この内積を**標準内積**という.

一方, 一つのベクトル空間に対しても異なる内積を定義することは可能であるし, 数ベクトル空間でない空間へも内積を定義できる.

例 1.3. (1) A を成分が正の実数である対角行列とする. このとき, $u, v \in K^n$ に対して

$$(u, v) = {}^t u A \overline{v}$$

は K^n 上の内積を定める. 特に, A が単位行列のとき, この内積は標準内積となる (それ以外のときは標準内積とは異なる内積).

(2) $K[x]_n$ によって, K 係数の n 次式以下の多項式全体の集合を表す (これは K 上 n 次元ベクトル空間). このとき, $f(x), g(x) \in V = K[x]_n$ に対して,

$$(f(x), g(x)) = \int_0^1 f(x)\overline{g(x)}\, dx$$

は V の計量ベクトル空間としての構造を与える. ($\overline{g(x)}$ は多項式に対する複素共役) ここで, 多項式の微分積分は形式的なものを考える.

以下, V を計量ベクトル空間とする.

次に, ベクトルの長さおよび直交性を定義しよう.

定義 1.4. (1) ベクトル v に対して, $\|v\| = \sqrt{(v, v)}$ を v の**ノルム** (長さ) という. ここで, $(v, v) \in \mathbb{R}$ であることに注意する. また, $\|v\| = 1$ のとき, v を**単位ベクトル**という. すぐにわかるように, ($v \neq 0$ のとき) $\dfrac{v}{\|v\|}$ は単位ベクトルである.

(2) ベクトル u, v が $(u, v) = 0$ を満たすとき, u と v は**直交**するといい, $u \perp v$ とかく. 簡単にわかるように, 互いに直交する非零なベクトル $v_1, \cdots, v_m$ は一次独立となる.

複素数 $\alpha = a + b\sqrt{-1}$ に対して, $|\alpha| = \sqrt{a^2 + b^2}$ で複素数の絶対値 (原点からの距離) を表す. 直接計算によって, 次のよく知られた公式を得ることができる.

事実 1.5. u, v をベクトルとすると, 次が成り立つ.

(1) (三平方の定理) $u \perp v$ ならば, $\|u + v\|^2 = \|u\|^2 + \|v\|^2$

(2) (シュワルツの不等式) $|(u, v)| \leq \|u\|\|v\|$

(3) (三角不等式) $\|u + v\| \leq \|u\| + \|v\|$

1.2 体積

この節の目標だった体積について考える.

まずは体積を求めるために必要な高さを導入する. 高さとは, 与えられた点と直線や平面との「距離」であり, 問題は直線や平面内のどの点を選べば「最短になるか」ということである. その点を探すために, “良い” 基底を選ぶことから始める.

定義-定理 1.6. ノルム 1 の互いに直交する基底を**正規直交基底**という. 任意の (有限次元) 計量ベクトル空間は必ず正規直交基底をもつ (**グラム–シュミットの正規直交化**, 後述).

「最短のルート」を定義し, 高さを導入する.

定義-定理 1.7. U を計量ベクトル空間 V の部分空間とし, $v_1, \cdots, v_m$ を U の正規直交基底とする[*3]. 写像 $\mathrm{pr}_U : V \to U$ を次で定義する:

$$\mathrm{pr}_U(v) = (v, v_1)v_1 + (v, v_2)v_2 + \cdots + (v, v_m)v_m.$$

このとき, 次が成り立つ:

(1) 写像 pr_U は線型写像である.
(2) v と $\mathrm{pr}_U(v)$ の距離 $\|v - \mathrm{pr}_U(v)\|$ は, v と U のベクトル u の距離 $\|v - u\|$ の中で最短である. つまり, v と U の距離 (最短) を定める.

そこで, v と U の距離 $\|v - \mathrm{pr}_U(v)\|$ を v から U への**高さ**とよび, $\mathrm{ht}_U(v)$ とかく. また, 線型写像 pr_U を U への**正射影**という.

注意 1.8. 線型写像 pr_U は U の正規直交基底の取り方に依らない (後述).

証明. (1) は自明. (2) を示す. すぐにわかるように, $v - \mathrm{pr}_U(v)$ は任意の U のベクトルと直交する; 実際に, u_i との内積を考えればよい. よって, 任意の $u \in U$ に対して,

$$\begin{aligned} \|v - u\|^2 &= \|(v - \mathrm{pr}_U(v)) + (\mathrm{pr}_U(v) - u)\|^2 \\ &= \|v - \mathrm{pr}_U(v)\|^2 + \|\mathrm{pr}_U(v) - u\|^2 \\ &\geq \|v - \mathrm{pr}_U(v)\|^2 \end{aligned}$$

ここで, 2 つ目の等号は三平方の定理から成り立つ. また, 内積の定義より, 等号成立は $u = \mathrm{pr}_U(v)$ のときに限る. □

[*3] V の内積を用いて U も計量ベクトル空間とみる.

以下, この部分節を通して, $K = \mathbb{R}$ とし, 標準内積による計量ベクトル空間 $V = \mathbb{R}^n$ を考える.

体積とは, 与えられた図形に対して, 一つ次元の “低い” 部分 (底辺や底面, “底”) と高さの積として計算される. 同様にして, 平行六面体の体積を次のように帰納的に定義する.

定義 1.9. ベクトル $v_1, \cdots, v_m$ で作られる平行六面体を P_m とおく. P_m の体積 $\mathrm{vol}(P_m)$ を次のように定義する:

① $m = 1$ のとき, $\mathrm{vol}(P_1) = \|v_1\|$;
② $m > 1$ のとき, $\mathrm{vol}(P_m) = \mathrm{vol}(P_{m-1}) \times \mathrm{ht}_{\langle P_{m-1} \rangle}(v_m)$.

ここで, $\langle P_{m-1} \rangle$ は P_{m-1} を拡張して得られる ($v_1, \cdots, v_{m-1}$ で生成される) V の部分空間である.

上の体積の定義によると, 体積は “底” P_{m-1} の取り方 (前から順に $v_1, \cdots, v_{m-1}$ を取り “底” とした) に依るように見えるが, 実はそうではない. (底辺や底面は自由に決めてよい.) 特に, 次のことがわかる.

定理 1.10. ベクトル $v_1, \cdots, v_m$ で作られる平行六面体を P とする. また, $n \times m$ 行列 A を $(v_1\ v_2\ \cdots\ v_m)$ で定義する[*4]. このとき, $\mathrm{vol}(P)^2 = \det({}^tAA)$ が成り立つ[*5]. 特に, $m = n$ のとき, $\mathrm{vol}(P) = |\det A|$.

証明. m に関する帰納法で示す.

- $m = 1$ のとき: $A = (v_1)$ に注意して,

$$\mathrm{vol}(P)^2 = \|v_1\|^2 = (v_1, v_1) = {}^tv_1v_1 = \det({}^tAA).$$

- $m > 1$ のとき: $U = \langle v_1, \cdots, v_{m-1} \rangle$ (P の “底”) とおく. また, $w = v_m - \mathrm{pr}_U(v_m)$ ($\|w\|$ が高さ) とし, $B = (v_1\ \cdots\ v_{m-1}\ w)$ とする. $\mathrm{pr}_U(v_m)$ の定義より, B の第 m 列に他の列の数倍をたすことで A が得られる; つまり, B の列に関して, 「ある特定の基本変形」を繰り返せば, A になる. また, この「ある特定の基本変形」に対応する基本行列の行列式は 1 である. よって, 行列式 1 のある正則行列 X (= ある

[*4] A は一般に正方行列でないため, A 自身の行列式はとれない.
[*5] A の列を入れ替えても当該行列式は変わらない.

特定の基本行列いくつかの積) が存在して, $A = BX$ となる. このとき,

$$\det({}^tAA) = \det({}^tX{}^tBBX) = \det {}^tX \cdot \det({}^tBB) \cdot \det X = \det({}^tBB).$$

ここで, $C = (v_1 \ \cdots \ v_{m-1})$ とおくと,

$${}^tBB = \begin{pmatrix} {}^tC \\ {}^tw \end{pmatrix} (C \quad w) = \begin{pmatrix} {}^tCC & {}^tCw \\ {}^twC & {}^tww \end{pmatrix} \overset{v_i \perp w}{=\!=} \begin{pmatrix} {}^tCC & 0 \\ 0 & {}^tww \end{pmatrix},$$

したがって, $\det({}^tBB) = \det({}^tCC) \cdot {}^tww = \det({}^tCC) \cdot \|w\|^2$. 帰納法の仮定より, $\det({}^tCC)$ は $v_1, \cdots, v_{m-1}$ で作られる平行六面体の体積 (P の "底") の 2 乗だから, 上の式の右辺は P の体積の 2 乗に等しい; つまり, $\mathrm{vol}(P)^2 = \det({}^tAA)$ を得る.

後半の主張は明らか. □

この部分節の最後に, 平行六面体の辺の長さが与えられたとき, その体積が最大値を取る条件を考えよう. 直感的には, 無駄がなくできるだけ "直立" しているときが最大になるはずである. 実際に, 部分空間 U に対して, 任意のベクトル v は $v = \mathrm{pr}_U(v) + (v - \mathrm{pr}_U(v))$ と表すことができるが, v と U の高さ $\|v - \mathrm{pr}_U(v)\|$ が最大となるのは $\mathrm{pr}_U(v) = 0$ となることが必要十分である. したがって, 次を得る.

定理 1.11. 各辺の長さが与えられた平行六面体が最大の体積をもつ必要十分条件は, 各辺が互いに直交していることである. この場合の平行六面体の体積は, 各辺の長さの積と一致する.

1.3 グラム–シュミットの正規直交化と直交補空間

上では, 平行六面体の体積を目標にできるだけ最短のルートを辿ってきた. ここでは, その補足として (当該箇所で省略した)「グラム–シュミットの正規直交化」および「直交補空間」について学ぶ.

以下, V を K 上の計量ベクトル空間とする.

「グラム–シュミットの正規直交化」とは, "良い" 基底を作るための方法である. ここでいう "良い" 基底とは, "いつも使うような" 基底を指す. つまり, 通常の平面図形や立体図形 (中高数学) においては, いわゆる x 軸, y 軸, z 軸を主軸として考えてきた. 一般のベクトル空間においても, このような基底 (正規直交基底, 定義 1.6) が取れると便利であることは間違いないだろう. 例えば, 任意のベクトル空間は数ベクトル空間 K^n と同型であるが, 正規直交基底を取ることでこの同型を構成すると, V の内積は K^n に標準内積と対応する. つまり, 次が成り立つ.

定理 1.12. ベクトル $v_1, \cdots, v_n$ を V の正規直交基底とし, 写像 $\varphi : V \to K^n$ を次で定義する: 任意の $v \in V$ に対して, $v = a_1v_1 + \cdots + a_nv_n$ と表したとき, $\varphi(v) = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$[*6].

このとき, 任意の $v, w \in V$ に対して, $(v, w)_V = (\varphi(v), \varphi(w))_{K^n}$ が成り立つ. ここで, $(-, ?)_V$ は V における内積, $(-, ?)_{K^n}$ は K^n における標準内積である.

与えられた基底 $v_1, \cdots, v_n$ から正規直交基底を構成するために, まずは前から順々に直交化し, 最後に正規化する. (正規化は簡単だから) 問題は直交化であるが, 感覚的には '無駄な箇所をひいていく' ように行う (2 次元でお絵かきしてみるとよいだろう). 実際の手順は次である:

グラム–シュミットの正規直交化

① $w_1 := v_1$ とおく.

② $w_2 := v_2 - \underbrace{\dfrac{(v_2, w_1)}{(w_1, w_1)} w_1}_{\text{無駄分}} \quad \rightsquigarrow \quad w_2 \perp w_1$

③ $w_3 := v_3 - \underbrace{\dfrac{(v_3, w_1)}{(w_1, w_1)} w_1}_{w_1\text{との無駄分}} - \underbrace{\dfrac{(v_3, w_2)}{(w_2, w_2)} w_2}_{w_2\text{との無駄分}} \quad \rightsquigarrow \quad w_3 \perp w_1,\ w_3 \perp w_2$

– ⓝ まで続ける.

– 最後に正規化 $\rightsquigarrow \quad \dfrac{w_i}{\|w_i\|}$

これを「グラム–シュミットの正規直交化」とよび, 新しく得られた $w_1, \cdots, w_n$ は正規直交基底となる. (基底になるところだけ証明が残っているが, 定義 1.4 参照) これによって, 定理 1.6 の証明が完了し, さらに, 定理 1.7 (高さを求めるとき) に必要な正規直交基底も得ることができる.

次に, 正射影の裏側を探る. 定理 1.7 においては, 部分空間 U の正規直交基底を取り, '無理矢理' 正射影を求め, 高さを計算した. 一方で, この正射影にはベクトル空間論としての重要な概念が隠れている. まずは, 部分空間の直和を導入する.

定義-定理 1.13. U, W を V の部分空間とする. (線型数学で学んだように) それらの和

[*6] この φ は同型な線型 写像 である.

$U+W$[*7]および共通部分 $U\cap W$ はまた, V の部分空間である. 特に, $V=U+W$ (U と W で全体を構成できる), かつ, $U\cap W=\{0\}$ (U と W が互いに干渉しない) とき, V は U と W の**直和**であるといい, $V=U\oplus W$ とかく. また, W を V における U の**補空間**という. このとき, U の V における補空間は必ず存在するが, 一意的ではない. さらに, V のすべてのベクトルは, U と W のベクトルの和として 一意的に 表せる (簡単).

補空間の存在は後に任せるとして, 一意的でないことを見てみよう.

例 1.14. $K=\mathbb{R}, V=\mathbb{R}^3$ とする. U を xy 平面, つまり, $U=\left\{\begin{pmatrix}x\\y\\z\end{pmatrix}\;\middle|\;z=0\right\}$ とする. このとき, 明らかに z 軸, つまり, $W_1=\left\{\begin{pmatrix}x\\y\\z\end{pmatrix}\;\middle|\;x=y=0\right\}$ は, U の V における補空間である: $V=U\oplus W_1$. 一方, $W_2=\left\{\begin{pmatrix}x\\y\\z\end{pmatrix}\;\middle|\;x=y=z\right\}$ $(\neq W_1)$ も U の補空間である. 実際, 任意にベクトル $\begin{pmatrix}x\\y\\z\end{pmatrix}$ を取ったとき, $\begin{pmatrix}x\\y\\z\end{pmatrix}=\underbrace{\begin{pmatrix}x-z\\y-z\\0\end{pmatrix}}_{U}+\underbrace{\begin{pmatrix}z\\z\\z\end{pmatrix}}_{W_2}\in U+W_2$ であるから, $V=U+W_2$ を得る. さらに, $U\cap W_2=\{0\}$ は明らか. よって, $V=U\oplus W_2$ となる.

補空間の存在について議論しよう. ここでは, “最も良い” 補空間を取ることにする. つまり, 与えられた部分空間 U と完全に直交するような 部分空間 を考える:

$$U^{\perp}=\{v\in V\mid \underset{(U\text{ の右側に突っ込んで内積が }0)}{\text{任意の } u\in U \text{ に対して}},\ (u,v)=0\}.$$

(これが V の部分空間であることは明らかだろう.) さらに, 次が成り立つ.

命題 1.15. V の部分空間 U に対して, 次が成り立つ.
(1) $V=U\oplus U^{\perp}$; (2) $(U^{\perp})^{\perp}=U$.

証明. (1) $V=U+U^{\perp}$ であること: $v\in V$ とする. U の正規直交基底を取り, その正射影 pr_U を考えると, $v=\mathrm{pr}_U(v)+(v-\mathrm{pr}_U(v))$ であり, $v-\mathrm{pr}_U(v)\in U^{\perp}$ となる.

$U\cap U^{\perp}=\{0\}$ であること: $u\in U\cap U^{\perp}$ とすると, 明らかに $(u,u)=0$. 内積の定義より, これは $u=0$ のときに限る.

(2) “$\supseteq$” $u\in U$ とする. このとき, 任意の $w\in U^{\perp}$ に対して, $(w,u)=\overline{(u,w)}=0$; ゆえに, $u\in(U^{\perp})^{\perp}$.

“$\subseteq$” $v\in(U^{\perp})^{\perp}$ とする. (1) より, $v=u+w$ $(u\in U, w\in U^{\perp})$ とかける. このとき,

$$(w,w)=\underbrace{(w,u)}_{\supseteq\text{ より }0}+(w,w)=\underbrace{(w,v)}_{v\in(U^{\perp})^{\perp}}=0,$$

[*7] ちなみに, $U+W=\{u+w\mid u\in U,\ w\in W\}$.

よって, 内積の定義より $w = 0$. したがって, $v = u \in U$. □

このように, $U^\perp$ は U に対して, とても良い補空間となる. そこで, $U^\perp$ を U の**直交補空間**とよぶ. このとき, 任意のベクトル v は $v = u + w$ $(u \in U, w \in U^\perp)$ と一意的に表すことができるため, 写像 $V \to U$ $(v \mapsto u)$ は well-defined であり, 線型性も簡単に確認できる. 一方, $v = \mathrm{pr}_U(v) + (v - \mathrm{pr}_U(v))$ とできるため, この線型写像と pr_U は一致する. また, pr_U が U の正規直交基底の取り方に依らないこともわかる (注意 1.8).

この節の最後に, $V = K^n$ (標準内積) の部分空間 U に対して, $U^\perp$ の実際の求め方について述べる.

まず, $U = \langle v_1, \cdots, v_m \rangle$ となるベクトル $v_1, \cdots, v_m$ を取る (例えば U の基底を取ればよい). また, $A = (v_1\ v_2\ \cdots\ v_m)$ ($n \times m$ 行列) とおき, $A^* = {}^t\overline{A}$ ($m \times n$ 行列)[*8]とする. このとき, 次が成り立つ.

命題 1.16. U の直交補空間は, $v \mapsto A^*v$ で定まる線型写像 $K^n \to K^m$ の核と一致する: $U^\perp = \{v \in K^n \mid A^*v = 0\}$. 特に, $\dim U^\perp = n - \mathrm{rank}\, A^*$ である.

証明. $v \in K^n,\ A^*v = 0 \Leftrightarrow {}^t\overline{v_i} \cdot v = 0 \Leftrightarrow {}^t v_i \cdot \overline{v} = 0 \Leftrightarrow (v_i, v) = 0 \Leftrightarrow u \in U^\perp$ □

2 有限体と群

この節では, q 個の元からなる有限体 $\mathbb{F} := \mathbb{F}_q$ から零を除いた集合 $\mathbb{F}^\times := \mathbb{F} \setminus \{0\}$ (乗法に関して群) の群構造を観察する. 明らかに $\mathbb{F}^\times$ はアーベル群であるが, さらに次のことがわかる.

定理 2.1. $\mathbb{F}^\times$ は位数 $q - 1$ の巡回群である.

$\phi : \mathbb{N} \to \mathbb{N}$ をオイラー関数とする.
上の定理を示すための準備をする.

補題 2.2. 正の整数 n に対して, $\displaystyle\sum_{d|n} \phi(d) = n$ が成り立つ.

証明. d を n の約数とすると, 巡回群 C_n は位数 d の部分群 H_d をただ一つもつ. 各 H_d は $\phi(d)$ 個の生成元をもつから主張が成り立つ. □

そこで, 定理 2.1 を証明しよう.

[*8] A の**随伴行列**とよぶ.

定理 2.1 の証明. d を $q-1$ の約数とし, アーベル群 $\mathbb{F}^\times$ が位数 d の元 a をもつと仮定する. 一方, $H_d = \{x \in \mathbb{F}^\times \mid x^d = 1\}$ は $\mathbb{F}^\times$ の部分群であり, a で生成された部分群 $\langle a \rangle$ を含む. $\mathbb{F}$ **上の** n **次方程式は高々** n **個の解をもつ**から, H_d の位数は高々 n である; $d = |\langle a \rangle| \leq |H_d| \leq d \rightsquigarrow H_d = \langle a \rangle \simeq C_d$.

$\mathbb{F}^\times$ の位数 d の元はすべて H_d に属し, それは $H_d \simeq C_d$ の生成元となる. その個数は $\phi(d)$ である.

($q-1$ の各約数 d に対して, 位数 d の元が存在するかどうか, 今のところ不明)

今, 補題 2.2 より $\displaystyle\sum_{d|q-1} \phi(d) = q-1$ が成り立つ. これは, 各 d に対して, 位数 d の元が必ず存在することを意味している. (もし "ない" と右辺は左辺より真に小さい.) 特に, $\mathbb{F}^\times$ は位数 $q-1$ の元をもつから, $\mathbb{F}^\times$ は巡回群である. □

3 組合せの公式

この節では, 教科書 [CVL, Exercise 1.5] における後半の主張に関する補足を与える. そこでの問は,

Exercise 1.5

t-(v,k,λ) デザイン $\mathcal{D} = (X, \mathcal{B})$ に対して, $v = 2k+1$ かつ t が偶数ならば,

$$\mathcal{E} := \left(X \cup \{\infty\},\ \left\{ \mathcal{B} \cup \{\infty\}, X \setminus B \;\middle|\; B \in \mathcal{B} \right\} \right)$$

は, $\mathcal{D}$ の拡大 (特に, 3-$(v+1, k+1, \lambda)$ デザイン) である.

ゼミで議論したように, 最後の問題は次である.

問題 3.1. 上の Exercise 1.5 の設定の下で,

$$\sum_{i=0}^{t} (-1)^i \binom{t+1}{i} \underbrace{\frac{(v-i)\cdots(v-t+1)}{(k-i)\cdots(k-t+1)}}_{t-i \text{ 個}} = 1$$

が成り立つことを示せ.

(自戒の念を込めて書くが) 当初, この問題を “代数的” に解くこと (特に式変形) を試みていたがまったくのミスリードだった[*9]. つまり, “デザイン論” の考え方がとても重要である. そこで, 教科書 [CVL, Exercise 1.5] の前半の主張から思い出そう[*10].

命題 3.2. $\mathcal{D} = (X, \mathcal{B})$ を t-(v, k, λ) デザインとし, $x_1, \cdots, x_{t+1}$ をその点とする. また, $x_1, \cdots, x_{t+1}$ をすべて含む $\mathcal{D}$ のブロックの個数を μ $(:= \mu_{\mathcal{D}})$ とおく. このとき, $x_1, \cdots, x_{t+1}$ のいずれも含まない $\mathcal{D}$ のブロックの個数は, $F + (-1)^{t+1}\mu$ である. ここで,

$$F\ (:= F_{\mathcal{D}}) = \lambda \cdot \sum_{i=0}^{t} (-1)^i \binom{t+1}{i} \frac{(v-i)\cdots(v-t+1)}{(k-i)\cdots(k-t+1)}$$

であり, この値は $\mathcal{D}$ のパラメータ t, v, k, λ だけで表される.

この命題において, $\dfrac{F}{\lambda}$ は特に, $\mathcal{D}$ のパラメータ t, v, k のみでかける. そこで,

$$c(t, v, k) := \sum_{i=0}^{t} (-1)^i \binom{t+1}{i} \frac{(v-i)\cdots(v-t+1)}{(k-i)\cdots(k-t+1)}$$

とおく.

さて, Exercise 1.5 を解決するために, 命題 3.2 を自明なデザインに適用する. 自明なデザインとは, v 個の元をもつ集合 X に対して, すべての k-部分集合をブロックとするデザインであり, 実際にこれは正の整数 t $(\leq k)$ に対して, t-(v, k, λ') デザインをなす (これこそ練習問題). ここで, $\lambda' = \binom{v-t}{k-t}$ である. これを $\mathcal{D}'$ で表す.

$x_1, \cdots, x_{t+1}$ を $\mathcal{D}'$ の点とすると, t が偶数のとき,

$$\begin{aligned}
\mu_{\mathcal{D}'} &\overset{(3.2)}{=\!=} \text{「}x_1, \cdots, x_{t+1} \text{ をすべて含む } \mathcal{D}' \text{ のブロックの個数」} \\
&\overset{easy}{=\!=} \tbinom{v-t-1}{k-t-1} \\
F_{\mathcal{D}'} - \mu_{\mathcal{D}'} &\overset{(3.2)}{=\!=} \text{「}x_1, \cdots, x_{t+1} \text{ をいずれも含まない } \mathcal{D}' \text{ のブロックの個数」} \\
&\overset{easy}{=\!=} \tbinom{v-t-1}{k}
\end{aligned}$$

(“easy” はどちらも自明なデザインの特徴から計算できる.) よって, $v = 2k + 1$ のとき,

$$F_{\mathcal{D}'} = \tbinom{v-t-1}{k-t-1} + \tbinom{v-t-1}{k} \overset{\text{高校}}{=\!=} \tbinom{v-t-1}{k+1} + \tbinom{v-t-1}{k} \overset{\text{高校}}{=\!=} \tbinom{v-t}{k+1} \overset{\text{高校}}{=\!=} \tbinom{v-t}{k-t} = \lambda',$$

[*9] ごめんなさい `m(_ _)m`

[*10] これはゼミ内で解決している.

したがって, ($c(t,v,k)$ はデザインの λ 以外のパラメータで決まり, 与えられたデザインと自明なデザインは同じ t,v,k をもつことに注意して)

$$c(t,v,k) \overset{\mathcal{D}'\text{で計算}}{=\!=\!=} \frac{F_{\mathcal{D}'}}{\lambda'} = 1.$$

このように, 問題 3.1 を解決することができた.

最後に, 得られた定理をまとめる.

定理 3.3. t-(v,k,λ) デザイン $\mathcal{D}=(X,\mathcal{B})$ に対して, $v=2k+1$ かつ t が偶数ならば,

$$\mathcal{E} := \left(X \cup \{\infty\},\ \left\{ \mathcal{B} \cup \{\infty\}, X \setminus B \;\middle|\; B \in \mathcal{B} \right\} \right)$$

は, $\mathcal{D}$ の拡大 (特に, 3-$(v+1,k+1,\lambda)$ デザイン) である.

あとがき

今回の敗因は, 当該式を “代数的に”(式変形で) 解こうとしたことだった. 一方, 得られた公式を特別なケースに適用して新たな公式を得ることは非常に重要でしばしば使われる手法であり, そこを見落としていた点はとても悔しさが残る (反省).

この問題は (筆者にとっては) 大変難しかったが, デザイン論に慣れている方にとっては “練習問題” なのだろうか. (教科書の当該箇所には, 「the number F depends only on the parameters of the design.」の一文があり, おそらくこれが重要なヒントなのだろうと推測した.) 当該教科書の “行間の広さ” に “溺れそう” になっているが, 引き続きデザイン論を楽しもうと思う. (ゼミのみんなも楽しんでもらえると嬉しい.)

4 オーバルとオーボイド

この節では[*11], [CVL, 例 1.42] の後半に現れるオーボイド (ovoid) について解説し, 再度, 例 1.42 について考える. まずは, 射影幾何 (射影空間) から思い出そう.

n を正の整数, q を素数ベキとし, V を $\mathbb{F} := \mathbb{F}_q$ 上の $n+1$ 次元ベクトル空間とする; つまり, $V=\mathbb{F}^{n+1}$ としてよい. このとき, V の部分空間全体からなる集合を $\mathrm{PG}(n,q)$ で表す. ここで注意すべきことは, V のベクトル (元) 自体を “点” と見るわけではなく, 部分空間を $\mathrm{PG}(n,q)$ の元と見ていることである. よって, 下に述べるように, 1 次元部分空間 が実際の “点” となる. (これにより, “射影” している感じが出る.)

[*11] 時と場合によって, 縦ベクトルと横ベクトルを用いる.

V の $i+1$ 次元部分空間 W を i **フラット**とよび, 特に,

- 0 フラット $\overset{\text{def}}{\iff}$ $\dim W = 1$ $\iff$ 点
- 1 フラット $\overset{\text{def}}{\iff}$ $\dim W = 2$ $\iff$ 直線
- 2 フラット $\overset{\text{def}}{\iff}$ $\dim W = 3$ $\iff$ 平面
- $n-1$ フラット $\overset{\text{def}}{\iff}$ $\dim W = n$ $\iff$ 超平面 (全体の 1 つ手前)

という. $\mathbb{F}$ は q 個の元からなる有限体なので, i フラットの個数は

$$\frac{\overbrace{(q^{n+1}-1)(q^{n+1}-q)\cdots(q^{n+1}-q^i)}^{i+1\text{ 個}}}{(q^{i+1}-1)(q^{i+1}-q)\cdots(q^{i+1}-q^i)}$$

である[*12]. 特に, 次がわかる.

- 点は $\dfrac{q^{n+1}-1}{q-1}$ 個ある.
- 直線は $\dfrac{(q^{n+1}-1)(q^{n+1}-q)}{(q^2-1)(q^2-q)}$ 本あり, それぞれの直線には $\dfrac{q^2-1}{q-1} = q+1$ 個の点が乗っている.
- 平面は $\dfrac{(q^{n+1}-1)(q^{n+1}-q)(q^{n+1}-q^2)}{(q^3-1)(q^3-q)(q^3-q^2)}$ 面あり, その上には $\dfrac{(q^3-1)(q^3-q)}{(q^2-1)(q^2-q)} = q^2+q+1$ 本の直線が存在する.

以下, 「直線上の点」などといったら, 上記の意味で用いる; つまり, 直線 $W(\dim W = 2)$ 上の点 $P(\dim P = 1)$ は実際には $P \subseteq W$.

"イメージ"

(ゼミで勉強したように) 以下の事実が成り立つ.

命題 4.1. $1 \leq i \leq n-1$ とする. X および $\mathcal{B}$ をそれぞれ, $\mathrm{PG}(n,q)$ の点および i フラット全体の集合とすると, $\mathcal{D} = (X, \mathcal{B})$ は 2 デザインをなす. 特に, $\mathcal{D}$ は

(1) $i = 1$: 2-$\left(\dfrac{q^{n+1}-1}{q-1},\ q+1,\ 1\right)$ デザイン (**点-直線デザイン**);

(2) $i = n-1$: 平方 2-$\left(\dfrac{q^{n+1}-1}{q-1},\ \dfrac{q^n-1}{q-1},\ \dfrac{q^{n-1}-1}{q-1}\right)$ デザイン (**点-超平面デザイン**)

[*12] $\mathbb{F}_q$ 上 $n+1$ 次元ベクトル空間の $i+1$ 次元部分空間の個数を求めるためには, 次の集合を 2 通りの数え方で数えればよい:

$\{(W, x_1, \cdots, x_{i+1}) \mid \dim W = i+1$ の部分空間 W, および, W の一次独立なベクトル $x_1, \cdots, x_{i+1}\}$.

である: $n=2$ のとき, これらは一致し, $\mathcal{D}$ は平方 2-$(q^2+q+1, q+1, 1)$ デザインとなる (位数 q の**射影平面**).

このような射影幾何における “卵型” を勉強することがこの節の目標である.

定義 4.2. どの 3 点も同一直線上にない

$$\begin{cases} q+1 \text{ 個の点からなる } \mathrm{PG}(2,q) \text{ の部分集合を}\textbf{オーバル} \\ q+2 \text{ 個の点からなる } \mathrm{PG}(2,q) \text{ の部分集合を}\textbf{超オーバル} \\ q^2+1 \text{ 個の点からなる } \mathrm{PG}(3,q) \text{ の部分集合を}\textbf{オーボイド} \end{cases}$$

という.

4.1 オーバル

まずは, 射影平面 $(n=2)$ における “卵” から観察する. $\mathrm{PG}(2,q)$ の点-直線は, シュタイナー $(\lambda=1)$ 平方 2 デザインをなすことを思い出しておこう.

- 点および直線は q^2+q+1 個;
- 直線上にはちょうど $q+1$ 個の点がある;
- 2 点を通る直線はちょうど 1 本である;
- 1 点を通る直線はちょうど $q+1$ 本ある.

定義 4.3. $\mathrm{PG}(2,q)$ の k **アーク** *(弧)* とは, どの 3 点も同一直線上にない k 個の点からなる部分集合である: オーバル $=q+1$ アーク.

$\mathrm{PG}(2,q)$ において k アーク $\mathcal{K}$ と直線が与えられたとき, その共有点の個数は 0, 1, 2 のいずれかである (3 点は同一直線上にないから); それぞれ, $\mathcal{K}$ の**外線**, **接線**, **割線**という.

オーバルの接線について次が観察される.

補題 4.4. オーバル $\mathcal{O}$ の各点において, ちょうど 1 本の接線が引ける.

証明. P を $\mathcal{O}$ 上の点とする. $\mathcal{O}$ は P 以外に q 個の点をもち, 各々と P を結ぶことでちょうど q 本の直線が引ける (いずれも一致しないことに注意). 一方, P を通る直線は $q+1$ 本存在するから, 先に取った直線以外に 1 本の直線があるはずである; それが接線. □

この部分節の主役はオーバルだが, 超オーバルについて次を述べておく.

補題 4.5. 超オーバルは接線をもたない.

証明. $\mathcal{H}$ を超オーバルとし, それ上の点 P において接線をもつと仮定する. $|\mathcal{H}| = q+2$ より, $\mathcal{H}$ は点 P 以外に $q+1$ 個の点をもち, そのそれぞれと点 P を結ぶことにより, ちょうど $q+1$ 本の直線が引ける ($\mathcal{H}$ は超オーバルだから, 同一直線上に 3 点はないことに注意). したがって, 点 P を通る直線は $q+2$ 本 (以上) 存在することになる. しかし, 点 P を通る直線はちょうど $q+1$ 本のみであるから, 矛盾する. □

実際に k アークを構成してみよう.

命題 4.6. 既約な 2 次形式 $f(x,y,z)$[*13]の零点全体からなる集合は, $\mathrm{PG}(2,q)$ の $q+1$ アーク (オーバル) をなす.

証明. 工事中 □

このように構成されるオーバルを**円錐曲線**とよぶ.

例 4.7. 2 次形式 $f(x,y,z) = y^2 + xz$ の零点[*14]は, $(-t^2, t, 1)$ $(t \in \mathbb{F})$ または $(1,0,0)$ であり, これらの全体は $q+1$ 点からなるアークである.

このように, $\mathrm{PG}(2,q)$ のオーバルは必ず存在する. 逆に, オーバルは (q が奇数のとき) 最大サイズのアークであることがわかる.

命題 4.8. q を奇数とする.

(1) $k > q+1$ となる k アークは存在しない.
(2) オーバル $\mathcal{O}$ 上にない点から $\mathcal{O}$ への接線は, 存在すればちょうど 2 本である.

証明. (1) 超オーバルが存在しないことを示せばよい (1 点抜けば一つ小さいアークができるから). 【背理法】$\mathcal{H}$ を $\mathrm{PG}(2,q)$ の超オーバルと仮定する. 補題 4.5 より, $\mathcal{H}$ 上にない点 Q を通る直線と $\mathcal{H}$ は 0 点または 2 点で交わる. よって, Q を通る直線たちは, $\mathcal{H}$ 上の点を 2 点ずつに分割する. ゆえに, $\mathcal{H}$ は偶数個の点をもつことになるが, $|\mathcal{H}| = q+2$ および q は奇数より, 矛盾する.

(2) $\mathcal{O}$ 上にない点 Q から $\mathcal{O}$ へ接線 ℓ が引けたとし, その接点を P とする. Q を通る直線たちは $\mathcal{O}$ を 1 点もしくは 2 点で分割するが, $|\mathcal{O}| = q+1$ は偶数であるから, そのうち

[*13] 2 次の項だけからなる多項式
[*14] スカラー倍を無視していることに注意

接線は (ℓ がすでにあるからそれを含め) 偶数本なければならない, つまり, ℓ 以外に少なくてもあと 1 本存在する; それを ℓ_Q とかく. ℓ 上の異なる点 Q, Q' を通る直線はただ 1 本 (シュタイナー 2 デザイン) より, $\ell_Q \neq \ell_{Q'}$ であることに注意する. さらに, 補題 4.4 より, $\mathcal{O}$ の各点における接線はただ 1 本だから, ℓ_Q たちは同一の接点を共有しない. よって, これら以外に ℓ 上の点から $\mathcal{O}$ へ接線を引くことはできず, ℓ および ℓ_Q のみが Q から $\mathcal{O}$ への接線である. □

次が知られている.

定理 4.9. q が奇数のとき, $\mathrm{PG}(2, q)$ のオーバルはすべて, 円錐曲線である.

証明. 工事中 □

4.2 オーボイド

この節の目標であったオーボイドについて考える. これは前部分節の 3 次元版であるから, 同様の流れで説明していこう. まずは $\mathrm{PG}(3, q)$ について次を思い出す.

- 点-超平面 (= 平面) は, 平方 2-$(q^3+q^2+q+1, q^2+q+1, q+1)$ デザイン;
- 直線は, $(q^2+1)(q^2+q+1)$ 本.

定義 4.10. どの 3 点も同一直線上にない k 個の点からなる $\mathrm{PG}(3, q)$ の部分集合を k **キャップ**という: オーボイド $= q^2+1$ キャップ.

k キャップと平面 (この場合, 超平面) との交わりは, その平面のアークであるから, その交点数は $q+1$ 以下である (命題 4.6 および 4.8).

次のように構成される q^2+1 キャップ (オーボイド) が代表的である.

命題 4.11. 既約な 2 次形式 $f(x, y, z, w)$ の零点全体からなる集合は, $\mathrm{PG}(3, q)$ の q^2+1 キャップ (オーボイド) をなす.

証明. 工事中 □

このように構成されるオーボイドを**楕円曲面**という.

例 4.12. 2 次形式 $f(x, y, z, w) = x^2 + xy + \delta y^2 - zw$ を考える. ここで, δ は $x^2+x+\delta$ が $\mathbb{F}$ 上既約となる $\mathbb{F}$ の元である. このとき, $f(x, y, z, w) = 0$ の開集合は,

$$\{(\alpha, \beta, \alpha^2 + \alpha\beta + \delta\beta^2, 1) \mid \alpha, \beta \in \mathbb{F}\} \cup \{(0, 0, 1, 0)\}$$

であり (スカラー倍を無視), オーボイドをなす.

これによって, $\mathrm{PG}(3,q)$ のオーボイドは必ず存在することがわかる. 逆に, オーボイドは $q>2$ のとき, 最大サイズのキャップであることがわかる.

命題 4.13. $q>2$ のとき, $k>q^2+1$ となる k キャップは存在しない. 特に, オーボイドと 2 点で交わる平面によるオーボイドの切断面はオーバルである.

証明. (i) q を奇数と仮定する. $\mathcal{O}$ を k キャップとし, それ上の異なる点 P,Q を取る. P,Q およびそれ以外の $\mathcal{O}$ の点は平面を張るから, 直線 PQ を通る 2 平面は $\mathcal{O}$ 上で P,Q のみと交わる. また, 直線 PQ を通る平面と $\mathcal{O}$ の交わりはアークをなす (最大でオーバル). よって, $k=|\mathcal{O}|\leq (\underset{\substack{\text{直線 } PQ \text{ を}\\ \text{通る平面}}}{q+1})(\underset{\substack{\text{オーバル}\\ (P,\,Q\ \text{以外})}}{q-1})+\underset{P,\,Q}{2}=q^2+1$. 特に, $k=q^2+1$ のとき, この不等式の等号が成立し, 切断面はすべてオーバルであることがわかる.

(ii) q が偶数の場合, 工事中. □

次を示すことが, この節の一つ目の目標である.

定理 4.14. $\mathcal{O}$ を $\mathrm{PG}(3,q)$ のオーボイドとし, $q>2$ を仮定する. このとき, 次が成り立つ.

(1) 点 P における $\mathcal{O}$ の接線全体は平面をなす;
(2) $\mathrm{PG}(3,q)$ における平面 q^3+q^2+q+1 個のうち, ちょうど q^2+1 個が $\mathcal{O}$ と 1 点で接し, その他 q^3+q 個の平面は $\mathcal{O}$ とオーバルで交わる;
(3) 特に, $\mathrm{PG}(3,q)$ の任意の平面は, $\mathcal{O}$ と 1 点または $q+1$ 点で交わる [CVL, 例 1.42].

証明. q を奇数とする; 偶数ケースは工事中.

(1) 点 P における異なる 2 接線 ℓ_1,ℓ_2 を取り, それらで張られる平面を π とおく. もし, π による $\mathcal{O}$ の切断面がオーバルならば, ℓ_1 および ℓ_2 はそのオーバルの接線でもある. このとき, 補題 4.4 より, $\ell_1=\ell_2$ となり矛盾する. よって, π は $\mathcal{O}$ とただ 1 点 P でのみ共有点をもち, π は P におけるすべての接線で張られる接平面であることがわかる.

(2) (1) より, $\mathcal{O}$ の各点 P における接平面はちょうど 1 つ (π のみ) である. したがって, $\mathcal{O}$ に接する面はちょうど q^2+1 個ある.

点 P を通る平面は, (点-超平面デザインを考えて) 全部で q^2+q+1 個あるが, そのうちの 1 面は π, 残りの q^2+q 個は $\mathcal{O}$ とオーバルで交わる. そのオーバルにおける $q+1$ 個の点で重複して平面を数えているから, $\mathcal{O}$ とオーバルで交わる平面は全部で, $\dfrac{(q^2+1)(q^2+q)}{q+1}=q^3+q$ 個存在することがわかる.

これらで $\mathrm{PG}(3,q)$ の平面はすべて尽きている. □

このように, 与えられたオーボイドによって, すべての平面は接平面 (ただ 1 点で交わる) または**割平面** (切断面がオーバル) に分けられる.

教科書では言及されていない (!) が, $q=2$ の場合, 定理 4.14(3) は成り立たない.

例 4.15. $\mathcal{O}$ を次の点からなる $\mathrm{PG}(3,2)$ の部分集合とする (スカラー倍は無視):

$$\mathcal{O} := \left\{ \begin{pmatrix} 1\\0\\0\\1 \end{pmatrix}, \begin{pmatrix} 0\\1\\0\\1 \end{pmatrix}, \begin{pmatrix} 0\\0\\1\\1 \end{pmatrix}, \begin{pmatrix} 1\\1\\0\\1 \end{pmatrix}, \begin{pmatrix} 0\\0\\0\\1 \end{pmatrix} \right\}.$$

これは $5 = 2^2+1$ 点からなり, $\mathrm{PG}(3,2)$ におけるオーバルであることが簡単にわかる. 一方, 3 つの単位ベクトル e_1, e_2, e_3 で張られた $\mathrm{PG}(3,2)$ の (超) 平面 W を考えると, 明らかに $\mathcal{O}$ と W は交わらない. (つまり, 交点数は 0.)

このように, $\mathrm{PG}(3,2)$ における最大サイズのキャップを考えるためには, q^2+1 では足りない. (この場合, 8 点必要. 後部分節を参照.)

上からわかるように, オーボイドからデザインを構成できる.

命題 4.16. $\mathcal{O}$ を $\mathrm{PG}(3,q)$ のオーボイドとする $(q>2)$. 割平面と $\mathcal{O}$ との交点全体の集合をブロックとし, その全体を $\mathcal{K}$ とおく. このとき, $(\mathcal{O},\mathcal{K})$ は 3-$(q^2+1, q+1, 1)$ デザインをなす. よって, これはある反転平面 (アフィン平面の拡大) と一致する.

この命題のように構成される反転平面を, **エッグライク**という. 知られている反転平面はすべてエッグライクである.

次が知られている; 定理 4.9 を参照.

定理 4.17. $\mathcal{O}$ を $\mathrm{PG}(3,q)$ のオーボイドとする $(q>2)$. このとき, すべての割平面と $\mathcal{O}$ との交点が円錐曲線であるならば, $\mathcal{O}$ は楕円曲面である. 特に, q が奇数ならば, すべてのオーボイドは楕円曲面である.

4.3 例 1.42 (再)

ここで, [CVL, 例 1.42] を再び観察しよう. そこでは, 2 つの方法 (1 つは命題 4.16) で構成した反転平面が同じデザインであることを言及している.

まずは, 構成に必要な群 $\mathrm{PGL}(2,q^2)$ について思い出す:

$$\mathrm{PGL}(2,q^2) := \left\{ f : X \to X \ \left(z \mapsto \frac{az+b}{cz+d} \right) \ \middle|\ a,b,c,d \in \mathbb{F}_{q^2}, ad-bc \neq 0 \right\}.$$

ここで, (特に $c \neq 0$ のとき) うまく定義されない点があるが, 次のように回避する:

- $c \neq 0$ のとき: $-\dfrac{d}{c} \mapsto \infty,\ \infty \mapsto \dfrac{a}{c}$;
- $c = 0$ のとき: $\infty \mapsto \infty$.

このとき, $f \in \mathrm{PGL}(2, q^2)$ は $X \to X$ の全単射を引き起こす. (よって, $\mathrm{PGL}(2, q^2)$ は群.)

一方, $\mathrm{PGL}(2, q^2)$ を次のように定義することもできる:

$$\begin{aligned} \mathrm{GL}(2, q^2) &:= \{A \in \mathrm{Mat}_2(\mathbb{F}_{q^2}) \mid \det A \neq 0\}; \\ Z(\mathrm{GL}(2, q^2)) &= \{aE \mid a \in \mathbb{F}_{q^2}^{\times}\}; \\ \mathrm{PGL}(2, q^2) &:= \mathrm{GL}(2, q^2)/Z(\mathrm{GL}(2, q^2)). \end{aligned}$$

ここで, $Z(-)$ は群 $-$ の中心, E は単位行列を表す. $|\mathrm{PGL}(2, q^2)| = (q^2-1)\cdot q^2 \cdot (q^2+1)$. このとき, $A \in \mathrm{PGL}(2, q^2)$ は, $V = \mathbb{F}_{q^2}^2$ ($\mathbb{F}_{q^2}$ 上 2 次元ベクトル空間) に関する $\mathrm{PG}(1, q^2)$ の点全体の集合 $X = \left\{ \binom{z}{1}, \binom{1}{0} \;\middle|\; z \in \mathbb{F}_{q^2} \right\}$ からそれ自身への全単射を引き起こす; 中心でわっていることにより, well-defined 性が担保される. つまり, $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \leftrightarrow f\ \left(z \mapsto \dfrac{az+b}{cz+d}\right)$ は, 上の 2 つの $\mathrm{PGL}(2, q^2)$ の間の同型写像を与える. 実際, $c \neq 0$ のとき,

$$\begin{aligned} f(z) \quad \rightsquigarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} z \\ 1 \end{pmatrix} &= \begin{pmatrix} az+b \\ cz+d \end{pmatrix} = \begin{cases} \begin{pmatrix} \frac{az+b}{cz+d} \\ 1 \end{pmatrix} & \left(z \neq -\dfrac{d}{c}\right) \rightsquigarrow \dfrac{az+b}{cz+d} \\ \begin{pmatrix} 1 \\ 0 \end{pmatrix} & \left(z = -\dfrac{d}{c}\right) \rightsquigarrow \infty \end{cases} \\ f(\infty) \quad \rightsquigarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} &= \begin{pmatrix} a \\ c \end{pmatrix} = \begin{pmatrix} \frac{a}{c} \\ 1 \end{pmatrix} \rightsquigarrow \frac{a}{c} \end{aligned}$$

ここで, $z = -\dfrac{d}{c}$ のとき, $az + b = -\dfrac{ad-bc}{c} \neq 0$ であることに注意する. 同様に, $c = 0$ のときも観察できる.

[CVL, 例 1.42] で構成されるもう一つの反転平面は次である.

例 4.18. $X := \mathbb{F}_{q^2} \cup \{\infty\}$ とする. また, 各 $f \in \mathrm{PGL}(2, q^2)$ に対して, $B_f := f(\mathbb{F}_q \cup \{\infty\})$ とおき, $\mathcal{B} := \{B_f\}$ と定義する. このとき, $(X, \mathcal{B})$ は 3-$(q^2+1, q+1, 1)$ デザインをなす.

証明. (ゼミでやったがもう一度確認する.)

$|X| = q^2 + 1$, また, f は全単射より $|B_f| = q + 1$ であることは明らか.

異なる 3 点 $s, t, u \in X = \mathbb{F}_{q^2} \cup \{\infty\}$ を取る.

- $s,t,u \in \mathbb{F}_{q^2}$ (つまり, いずれも ∞ でない) とき: $f := \begin{pmatrix} -u(t-s) & s(t-u) \\ -(t-s) & t-u \end{pmatrix}$ とおくと, $\det f \neq 0$ であり, $0 \mapsto s,\ 1 \mapsto t,\ \infty \mapsto u$ となるから $s,t,u \in B_f$ を得る.
- s,t,u のうち, いずれかが ∞ のとき ($u = \infty$ としてよい): $f := \begin{pmatrix} t-s & s \\ 0 & 1 \end{pmatrix}$ とすると, 上と同様に, $0 \mapsto s,\ 1 \mapsto t,\ \infty \mapsto u\ (=\infty)$ より $s,t,u \in B_f$ となる.

このように, 任意の異なる 3 点を含むブロックの存在がわかる.

最後に, 異なる 3 点 $s,t,u \in X$ を含むブロックがただ一つであること ($\lambda = 1$) を示そう. つまり, $h \in \mathrm{PGL}(2,q^2)$ に対して, $s,t,u \in B_h$ ならば, 上で構成したような f によって $B_h = B_f$ となることをいえばよい. $s,t,u \in B_h$ より, $\alpha,\beta,\gamma \in \mathbb{F}_q \cup \{\infty\}$ が存在して $h(\alpha) = s, h(\beta) = t, h(\gamma) = u$ となる. 一方, 上の構成法を α,β,γ に適用すれば, $0 \mapsto \alpha,\ 1 \mapsto \beta,\ \infty \mapsto \gamma$ となる $\sigma \in \mathrm{PGL}(2,q^2)$ が得られるが, σ の成分はすべて $\mathbb{F}_q$ からなるので $B_\sigma = B_1$ となることがわかる. したがって, $B_h = B_{h\sigma}$ より, h は初めから $0 \mapsto s,\ 1 \mapsto t,\ \infty \mapsto u\ \cdots(*)$ としてよい. そこで, $h = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ とおき, $(*)$ を満たすように a,b,c,d を計算すると, h と f は中心を無視して (スカラー倍を除いて) 一致することがわかる. ゆえに, $B_f = B_h$ を得る. □

教科書では次が述べられている.

命題 4.19. 例 4.18 で構成されたデザイン $(X,\mathcal{B})$ と, ある楕円曲面から得られる反転平面 (命題 4.16) は一致する.

証明. (i) 例 4.18 $\rightsquigarrow$ 命題 4.16: $(X,\mathcal{B})$ を例 4.18 のように得られるデザインとする. このとき, $X = \mathbb{F}_{q^2} \cup \{\infty\}$ の元を次のように読み替える:

$$\begin{array}{ccc} \alpha + \beta\lambda & \longleftrightarrow & (\alpha,\beta,\alpha^2+\alpha\beta+\delta\beta^2,1) \\ \infty & \longleftrightarrow & (0,0,1,0) \end{array}$$

ここで, δ は $x^2+x+\delta$ が $\mathbb{F}_q$ 上既約となるような $\mathbb{F}_q$ の元とする. この対応の右側の点たち (全部で q^2+1 個) は, 2 次形式 $x^2+xy+\delta y^2-zw$ の零点全体の集合 $\mathcal{O}$ であるから (例 4.12), これは $PG(3,q)$ の楕円曲面をなす (スカラー倍を無視していることに注意).

また, $g(x,y)$ を既約な 2 元 2 次形式とする; これの零点 (x,y) は $(0,0)$ のみであること

に注意する. このとき, $X = \mathbb{F}_{q^2} \cup \{\infty\}$ の元を次のように読み替える:

$$\begin{array}{ccc} \alpha + \beta\lambda & \longleftrightarrow & (\alpha, \beta, g(\alpha, \beta), 1) \\ \infty & \longleftrightarrow & (0, 0, 1, 0) \end{array}$$

これらが既約な 2 次形式 $f(x, y, z, w) = g(x, y) - zw$ の零点であることは簡単にわかるから, それら全体 (全部で $q^2 + 1$ 点) の集合 $\mathcal{O}$ は $\mathrm{PG}(3, q)$ の楕円曲面をなす (スカラー倍を無視していることに注意).

以下, $\mathrm{PGL}(2, q^2)$ の作用を考えるために, $\mathrm{PG}(3, q)$ を $\mathbb{F}_q$ 上 4 次元ベクトル空間 $\mathbb{F}_q^4$ または $\mathbb{F}_{q^2}^2$ に関する射影空間とみなす (適宜使い分ける): $(x, y, z, w) \leftrightarrow (x + y\lambda, w + z\lambda)$ で読み替える. $B := \{(\alpha, 0, g(\alpha, 0), 1),\ (0, 0, 1, 0) \mid \alpha \in \mathbb{F}_q\}$ とし, $\mathcal{B} = \{B_f \mid f \in \mathrm{PGL}(2, q^2)\}$ が命題 4.16 における $\mathcal{K}$ と一致することを示す.

- B は割平面 $y = 0$ と楕円曲面 $\mathcal{O}$ との交点全体である.

□

4.4 高次元化 $n \geq 4$

オーバロイド

参考文献

[CVL] P. J. Cameron and J. H. van Lint, Designs, graphs, codes and theire links. London Mathematical Society Student Texts, **22**. *Cambridge University Press, Cambridge*, 1991.