

離散数理工学 第 6 回

離散代数 : 有限幾何

岡本 吉央

okamotoy@uec.ac.jp

電気通信大学

2023 年 11 月 21 日

最終更新 : 2023 年 11 月 13 日 13:20

今日の目標

有限射影平面について次ができるようになる

- ▶ 有限体を用いて構成できるようになる
- ▶ 基本的な性質を証明できるようになる

目次

- ① 有限射影平面：例
- ② 有限射影平面：構成
- ③ 有限射影平面：一般
- ④ 今日のまとめ

問題：次の性質を満たす集合の集合は存在するか？

正整数 m, q , 有限集合 X , $|X| = v$

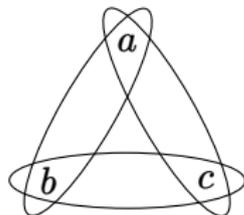
問題

m 個の集合 $A_1, A_2, \dots, A_m \subseteq X$ で次を満たすものは存在するか？

- ▶ $|A_1| = |A_2| = \dots = |A_m| = q + 1$
- ▶ 任意の異なる $i, j \in \{1, 2, \dots, m\}$ に対して $x \in A_i \cap A_j$ となる $x \in X$ が一意に存在する
- ▶ 任意の異なる $x, y \in X$ に対して $x, y \in A_i$ となる $i \in \{1, 2, \dots, m\}$ が一意に存在する

例： $X = \{a, b, c\}$, $v = 3$, $m = 3$, $q = 1$

$$A_1 = \{a, b\}, A_2 = \{a, c\}, A_3 = \{b, c\}$$



これをなぜ考えるのか？

正整数 m, q , 有限集合 X , $|X| = v$

問題

m 個の集合 $A_1, A_2, \dots, A_m \subseteq X$ で次を満たすものは存在するか？

- ▶ $|A_1| = |A_2| = \dots = |A_m| = q + 1$
- ▶ 任意の異なる $i, j \in \{1, 2, \dots, m\}$ に対して $x \in A_i \cap A_j$ となる $x \in X$ が一意に存在する
- ▶ 任意の異なる $x, y \in X$ に対して $x, y \in A_i$ となる $i \in \{1, 2, \dots, m\}$ が一意に存在する

X を「点の集合」、 A_i を「直線」だと思つと…

- ▶ 異なる 2 直線は 1 点で交わる
- ▶ 異なる 2 点を通る直線は 1 つ

⇨ 点と直線の関係を表しているように見える

これをなぜ考えるのか？

正整数 m, q , 有限集合 X , $|X| = v$

問題

m 個の集合 $A_1, A_2, \dots, A_m \subseteq X$ で次を満たすものは存在するか？

- ▶ $|A_1| = |A_2| = \dots = |A_m| = q + 1$
- ▶ 任意の異なる $i, j \in \{1, 2, \dots, m\}$ に対して $x \in A_i \cap A_j$ となる $x \in X$ が一意に存在する
- ▶ 任意の異なる $x, y \in X$ に対して $x, y \in A_i$ となる $i \in \{1, 2, \dots, m\}$ が一意に存在する

例： $q = 2$

今から行うこと

正整数 m, q , 有限集合 X , $|X| = v$

問題

m 個の集合 $A_1, A_2, \dots, A_m \subseteq X$ で次を満たすものは存在するか？

- ▶ $|A_1| = |A_2| = \dots = |A_m| = q + 1$
- ▶ 任意の異なる $i, j \in \{1, 2, \dots, m\}$ に対して $x \in A_i \cap A_j$ となる $x \in X$ が一意に存在する
- ▶ 任意の異なる $x, y \in X$ に対して $x, y \in A_i$ となる $i \in \{1, 2, \dots, m\}$ が一意に存在する

今から行うこと

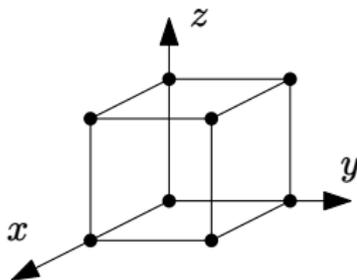
有限体を使って, この問題を部分的に解決する

今回は, $+$, \cdot を単に $+$, \cdot と書き, \cdot はよく省略する

射影平面：例 — 考える空間は $(\mathbb{Z}/2\mathbb{Z})^3$

- ▶ $(\mathbb{Z}/2\mathbb{Z})^3$ を考える

$$(\mathbb{Z}/2\mathbb{Z})^3 = \{(0, 0, 0), (1, 0, 0), (0, 1, 0), (0, 0, 1), (1, 1, 0), (1, 0, 1), (0, 1, 1), (1, 1, 1)\}$$



- ▶ $(\mathbb{Z}/2\mathbb{Z})^3$ は線形空間 (和とスカラー倍がとれる)

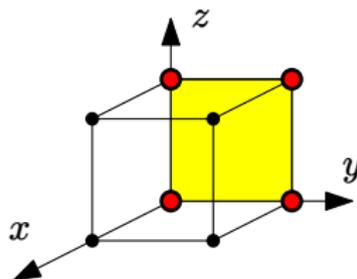
射影平面：例 — $(\mathbb{Z}/2\mathbb{Z})^3$ における平面

- ▶ $(\mathbb{Z}/2\mathbb{Z})^3$ において, 原点 $(0, 0, 0)$ を通る平面は,
 $(a, b, c) \in (\mathbb{Z}/2\mathbb{Z})^3 - \{0\}$ を使って

$$\{(x, y, z) \mid ax + by + cz = 0\}$$

と書ける

- ▶ 異なる (a, b, c) に対して, 異なる平面が得られる



$$\{(x, y, z) \mid x = 0\} = \{(0, 0, 0), (0, 1, 0), (0, 0, 1), (0, 1, 1)\}$$

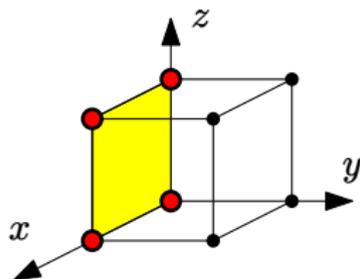
射影平面：例 — $(\mathbb{Z}/2\mathbb{Z})^3$ における平面

- ▶ $(\mathbb{Z}/2\mathbb{Z})^3$ において, 原点 $(0, 0, 0)$ を通る平面は,
 $(a, b, c) \in (\mathbb{Z}/2\mathbb{Z})^3 - \{0\}$ を使って

$$\{(x, y, z) \mid ax + by + cz = 0\}$$

と書ける

- ▶ 異なる (a, b, c) に対して, 異なる平面が得られる



$$\{(x, y, z) \mid y = 0\} = \{(0, 0, 0), (0, 0, 1), (1, 0, 0), (1, 0, 1)\}$$

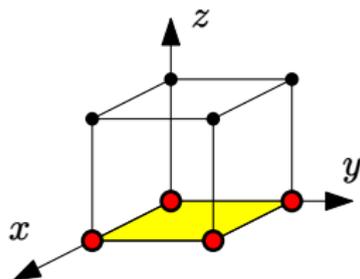
射影平面：例 — $(\mathbb{Z}/2\mathbb{Z})^3$ における平面

- ▶ $(\mathbb{Z}/2\mathbb{Z})^3$ において, 原点 $(0, 0, 0)$ を通る平面は,
 $(a, b, c) \in (\mathbb{Z}/2\mathbb{Z})^3 - \{0\}$ を使って

$$\{(x, y, z) \mid ax + by + cz = 0\}$$

と書ける

- ▶ 異なる (a, b, c) に対して, 異なる平面が得られる



$$\{(x, y, z) \mid z = 0\} = \{(0, 0, 0), (1, 0, 0), (0, 1, 0), (1, 1, 0)\}$$

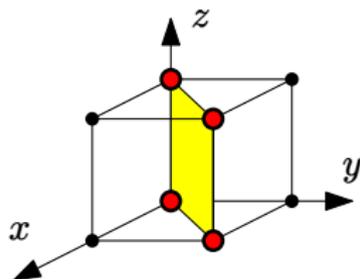
射影平面：例 — $(\mathbb{Z}/2\mathbb{Z})^3$ における平面

- ▶ $(\mathbb{Z}/2\mathbb{Z})^3$ において, 原点 $(0, 0, 0)$ を通る平面は,
 $(a, b, c) \in (\mathbb{Z}/2\mathbb{Z})^3 - \{0\}$ を使って

$$\{(x, y, z) \mid ax + by + cz = 0\}$$

と書ける

- ▶ 異なる (a, b, c) に対して, 異なる平面が得られる



$$\{(x, y, z) \mid x + y = 0\} = \{(0, 0, 0), (0, 0, 1), (1, 1, 0), (1, 1, 1)\}$$

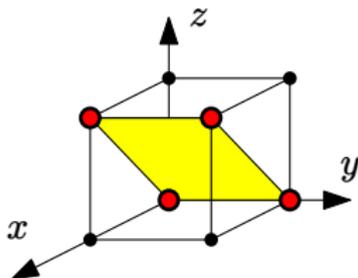
射影平面：例 — $(\mathbb{Z}/2\mathbb{Z})^3$ における平面

- ▶ $(\mathbb{Z}/2\mathbb{Z})^3$ において, 原点 $(0, 0, 0)$ を通る平面は,
 $(a, b, c) \in (\mathbb{Z}/2\mathbb{Z})^3 - \{0\}$ を使って

$$\{(x, y, z) \mid ax + by + cz = 0\}$$

と書ける

- ▶ 異なる (a, b, c) に対して, 異なる平面が得られる



$$\{(x, y, z) \mid x + z = 0\} = \{(0, 0, 0), (0, 1, 0), (1, 0, 1), (1, 1, 1)\}$$

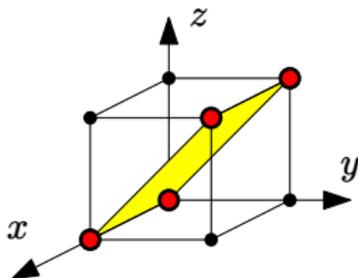
射影平面：例 — $(\mathbb{Z}/2\mathbb{Z})^3$ における平面

- ▶ $(\mathbb{Z}/2\mathbb{Z})^3$ において, 原点 $(0, 0, 0)$ を通る平面は,
 $(a, b, c) \in (\mathbb{Z}/2\mathbb{Z})^3 - \{0\}$ を使って

$$\{(x, y, z) \mid ax + by + cz = 0\}$$

と書ける

- ▶ 異なる (a, b, c) に対して, 異なる平面が得られる



$$\{(x, y, z) \mid y + z = 0\} = \{(0, 0, 0), (1, 0, 0), (0, 1, 1), (1, 1, 1)\}$$

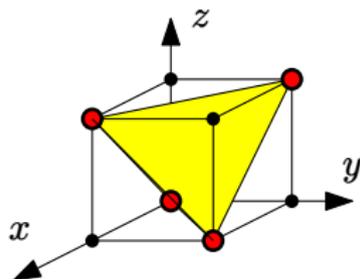
射影平面：例 — $(\mathbb{Z}/2\mathbb{Z})^3$ における平面

- ▶ $(\mathbb{Z}/2\mathbb{Z})^3$ において, 原点 $(0, 0, 0)$ を通る平面は,
 $(a, b, c) \in (\mathbb{Z}/2\mathbb{Z})^3 - \{0\}$ を使って

$$\{(x, y, z) \mid ax + by + cz = 0\}$$

と書ける

- ▶ 異なる (a, b, c) に対して, 異なる平面が得られる



$$\{(x, y, z) \mid x + y + z = 0\} = \{(0, 0, 0), (1, 1, 0), (1, 0, 1), (0, 1, 1)\}$$

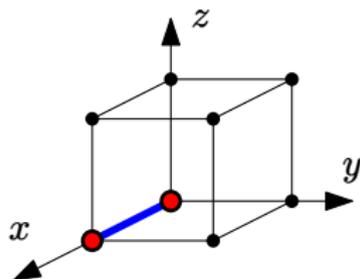
射影平面：例 — $(\mathbb{Z}/2\mathbb{Z})^3$ における直線

- ▶ $(\mathbb{Z}/2\mathbb{Z})^3$ において、原点 $(0, 0, 0)$ を通る直線は、 $(a, b, c) \in (\mathbb{Z}/2\mathbb{Z})^3 - \{0\}$ を使って

$$\{(x, y, z) \mid \text{ある } k \in \mathbb{Z}/2\mathbb{Z} \text{ が存在して, } x = ka, y = kb, z = kc\}$$

と書ける

- ▶ 異なる (a, b, c) に対して、異なる直線が得られる



$$\{(k, 0, 0) \mid k \in \mathbb{Z}/2\mathbb{Z}\} = \{(0, 0, 0), (1, 0, 0)\}$$

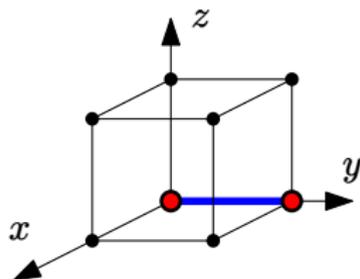
射影平面：例 — $(\mathbb{Z}/2\mathbb{Z})^3$ における直線

- ▶ $(\mathbb{Z}/2\mathbb{Z})^3$ において、原点 $(0, 0, 0)$ を通る直線は、 $(a, b, c) \in (\mathbb{Z}/2\mathbb{Z})^3 - \{0\}$ を使って

$$\{(x, y, z) \mid \text{ある } k \in \mathbb{Z}/2\mathbb{Z} \text{ が存在して, } x = ka, y = kb, z = kc\}$$

と書ける

- ▶ 異なる (a, b, c) に対して、異なる直線が得られる



$$\{(0, k, 0) \mid k \in \mathbb{Z}/2\mathbb{Z}\} = \{(0, 0, 0), (0, 1, 0)\}$$

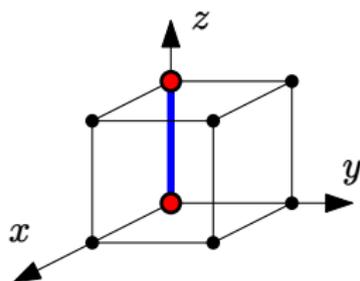
射影平面：例 — $(\mathbb{Z}/2\mathbb{Z})^3$ における直線

- ▶ $(\mathbb{Z}/2\mathbb{Z})^3$ において, 原点 $(0, 0, 0)$ を通る直線は,
 $(a, b, c) \in (\mathbb{Z}/2\mathbb{Z})^3 - \{0\}$ を使って

$$\{(x, y, z) \mid \text{ある } k \in \mathbb{Z}/2\mathbb{Z} \text{ が存在して, } x = ka, y = kb, z = kc\}$$

と書ける

- ▶ 異なる (a, b, c) に対して, 異なる直線が得られる



$$\{(0, 0, k) \mid k \in \mathbb{Z}/2\mathbb{Z}\} = \{(0, 0, 0), (0, 0, 1)\}$$

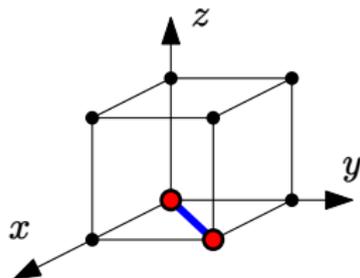
射影平面：例 — $(\mathbb{Z}/2\mathbb{Z})^3$ における直線

- ▶ $(\mathbb{Z}/2\mathbb{Z})^3$ において、原点 $(0, 0, 0)$ を通る直線は、 $(a, b, c) \in (\mathbb{Z}/2\mathbb{Z})^3 - \{0\}$ を使って

$$\{(x, y, z) \mid \text{ある } k \in \mathbb{Z}/2\mathbb{Z} \text{ が存在して, } x = ka, y = kb, z = kc\}$$

と書ける

- ▶ 異なる (a, b, c) に対して、異なる直線が得られる



$$\{(k, k, 0) \mid k \in \mathbb{Z}/2\mathbb{Z}\} = \{(0, 0, 0), (1, 1, 0)\}$$

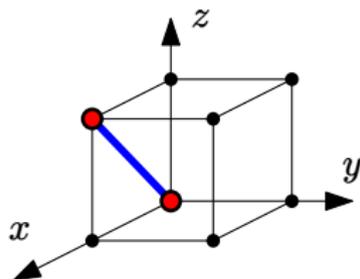
射影平面：例 — $(\mathbb{Z}/2\mathbb{Z})^3$ における直線

- ▶ $(\mathbb{Z}/2\mathbb{Z})^3$ において、原点 $(0, 0, 0)$ を通る直線は、 $(a, b, c) \in (\mathbb{Z}/2\mathbb{Z})^3 - \{0\}$ を使って

$$\{(x, y, z) \mid \text{ある } k \in \mathbb{Z}/2\mathbb{Z} \text{ が存在して, } x = ka, y = kb, z = kc\}$$

と書ける

- ▶ 異なる (a, b, c) に対して、異なる直線が得られる



$$\{(k, 0, k) \mid k \in \mathbb{Z}/2\mathbb{Z}\} = \{(0, 0, 0), (1, 0, 1)\}$$

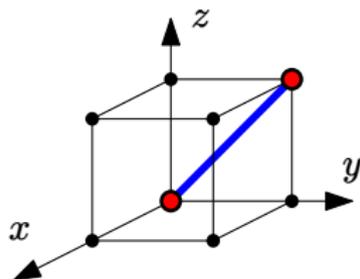
射影平面：例 — $(\mathbb{Z}/2\mathbb{Z})^3$ における直線

- ▶ $(\mathbb{Z}/2\mathbb{Z})^3$ において、原点 $(0, 0, 0)$ を通る直線は、 $(a, b, c) \in (\mathbb{Z}/2\mathbb{Z})^3 - \{0\}$ を使って

$$\{(x, y, z) \mid \text{ある } k \in \mathbb{Z}/2\mathbb{Z} \text{ が存在して, } x = ka, y = kb, z = kc\}$$

と書ける

- ▶ 異なる (a, b, c) に対して、異なる直線が得られる



$$\{(0, k, k) \mid k \in \mathbb{Z}/2\mathbb{Z}\} = \{(0, 0, 0), (0, 1, 1)\}$$

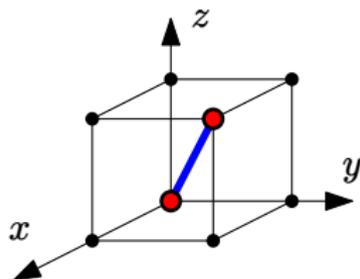
射影平面：例 — $(\mathbb{Z}/2\mathbb{Z})^3$ における直線

- ▶ $(\mathbb{Z}/2\mathbb{Z})^3$ において、原点 $(0, 0, 0)$ を通る直線は、 $(a, b, c) \in (\mathbb{Z}/2\mathbb{Z})^3 - \{0\}$ を使って

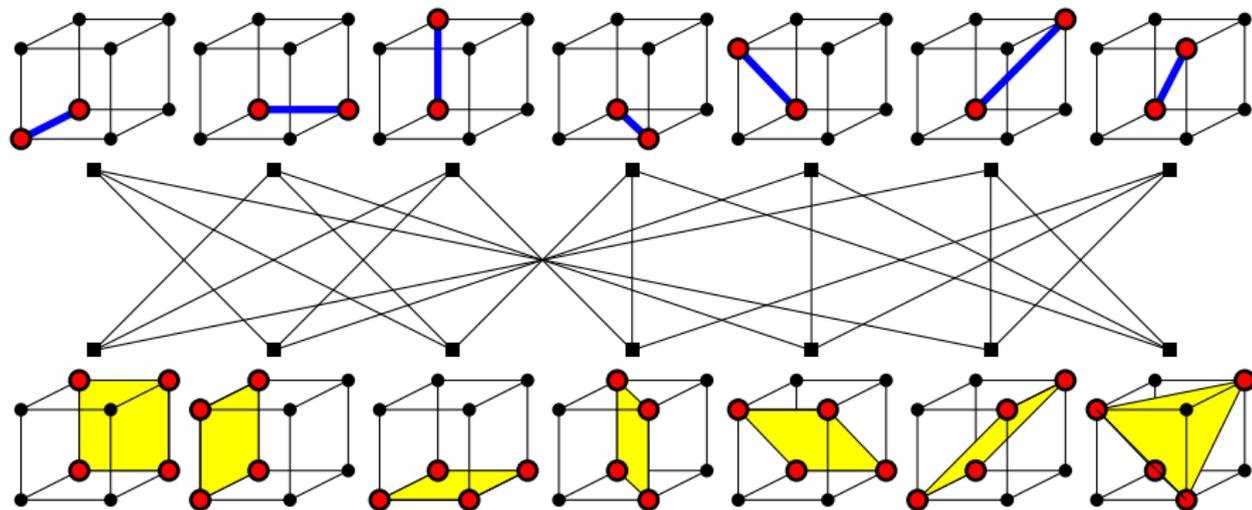
$$\{(x, y, z) \mid \text{ある } k \in \mathbb{Z}/2\mathbb{Z} \text{ が存在して, } x = ka, y = kb, z = kc\}$$

と書ける

- ▶ 異なる (a, b, c) に対して、異なる直線が得られる

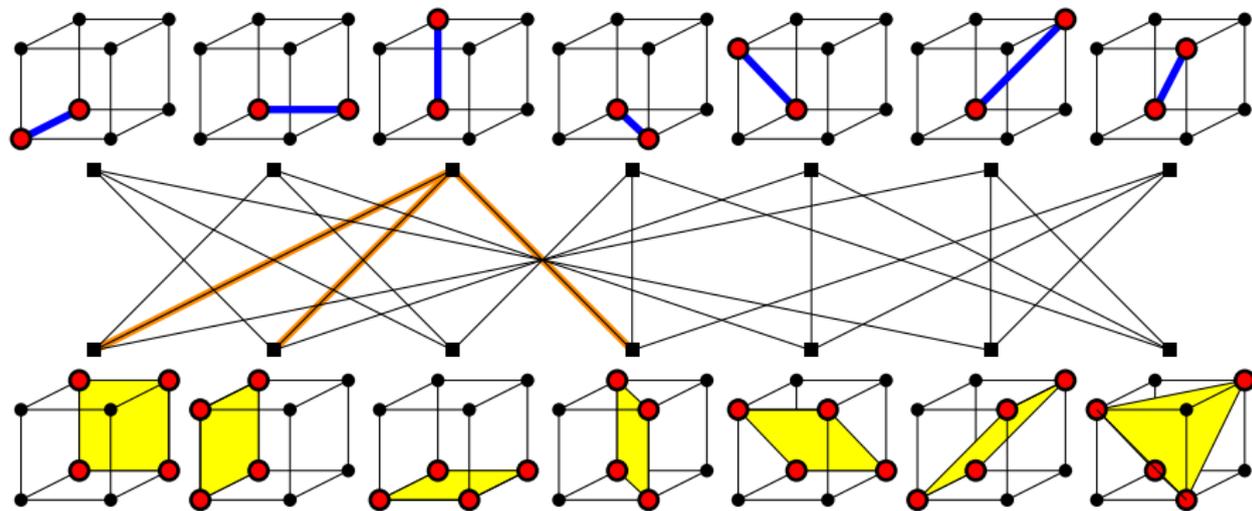


$$\{(k, k, k) \mid k \in \mathbb{Z}/2\mathbb{Z}\} = \{(0, 0, 0), (1, 1, 1)\}$$

射影平面：例 — $(\mathbb{Z}/2\mathbb{Z})^3$ における直線と平面の接続関係

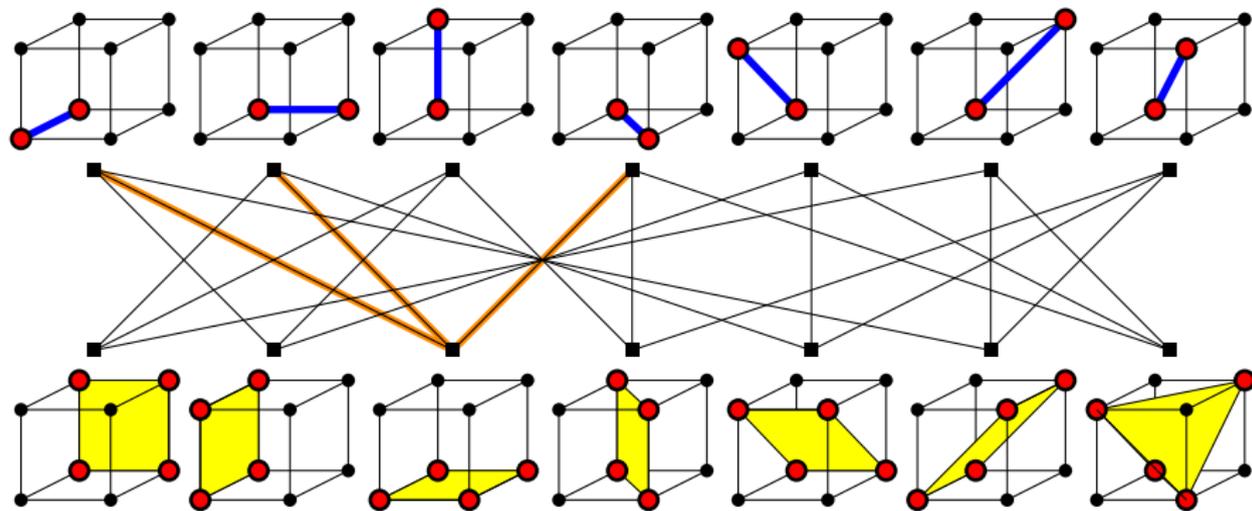
観察

- ▶ どの直線も 3 つの平面に含まれる
- ▶ どの平面も 3 つの直線を含む
- ▶ 2 つの平面に含まれる直線はちょうど 1 つ
- ▶ 2 つの直線を含む平面はちょうど 1 つ

射影平面：例 — $(\mathbb{Z}/2\mathbb{Z})^3$ における直線と平面の接続関係

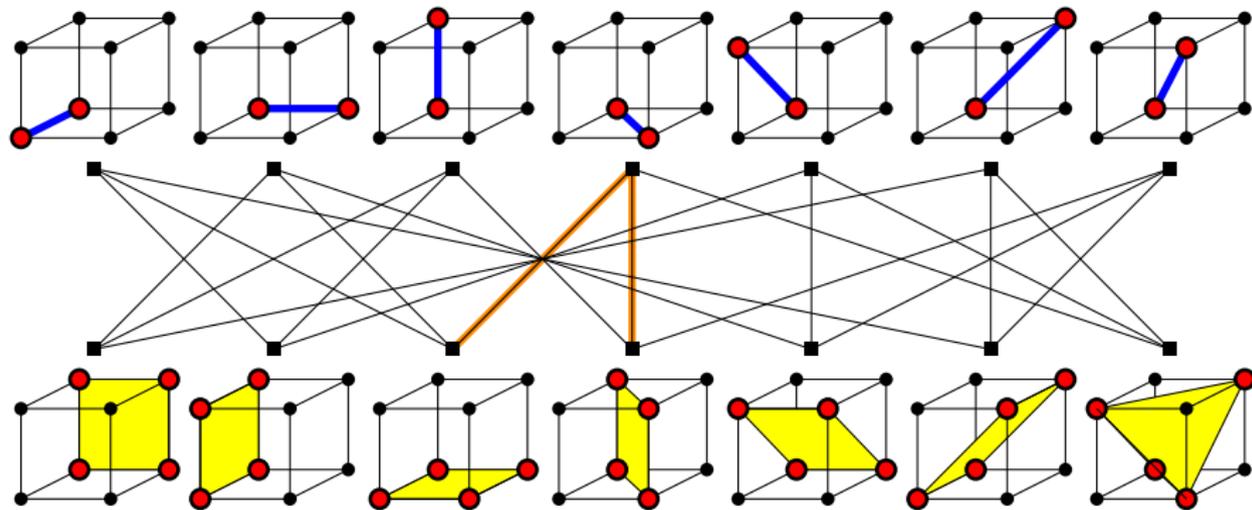
観察

- ▶ どの直線も 3 つの平面に含まれる
- ▶ どの平面も 3 つの直線を含む
- ▶ 2 つの平面に含まれる直線はちょうど 1 つ
- ▶ 2 つの直線を含む平面はちょうど 1 つ

射影平面：例 — $(\mathbb{Z}/2\mathbb{Z})^3$ における直線と平面の接続関係

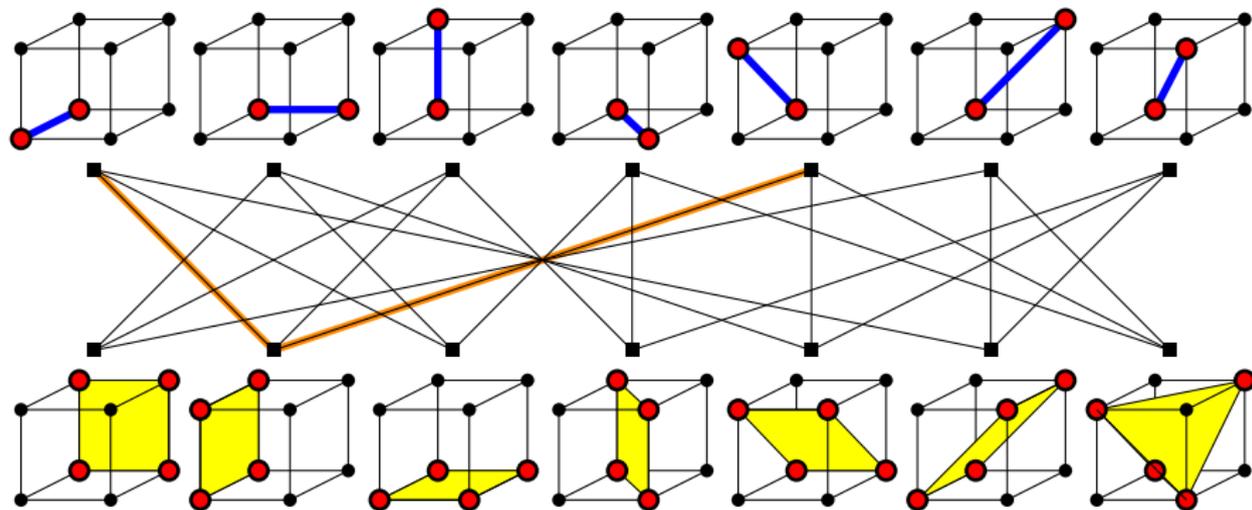
観察

- ▶ どの直線も 3 つの平面に含まれる
- ▶ どの平面も 3 つの直線を含む
- ▶ 2 つの平面に含まれる直線はちょうど 1 つ
- ▶ 2 つの直線を含む平面はちょうど 1 つ

射影平面：例 — $(\mathbb{Z}/2\mathbb{Z})^3$ における直線と平面の接続関係

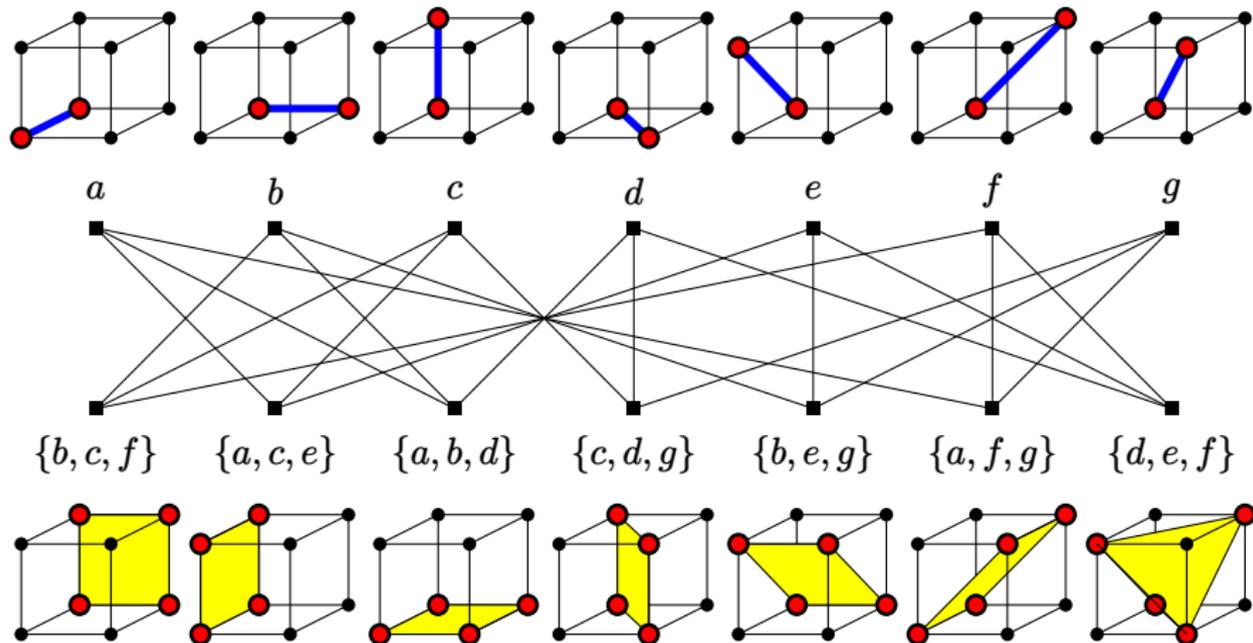
観察

- ▶ どの直線も 3 つの平面に含まれる
- ▶ どの平面も 3 つの直線を含む
- ▶ 2 つの平面に含まれる直線はちょうど 1 つ
- ▶ 2 つの直線を含む平面はちょうど 1 つ

射影平面：例 — $(\mathbb{Z}/2\mathbb{Z})^3$ における直線と平面の接続関係

観察

- ▶ どの直線も 3 つの平面に含まれる
- ▶ どの平面も 3 つの直線を含む
- ▶ 2 つの平面に含まれる直線はちょうど 1 つ
- ▶ 2 つの直線を含む平面はちょうど 1 つ

射影平面：例 — $q = 2$ のときの構成法

$v = 7, m = 7, q = 2$ の場合の構成になっている

目次

- ① 有限射影平面：例
- ② 有限射影平面：構成
- ③ 有限射影平面：一般
- ④ 今日のまとめ

\mathbb{F}_q 上の射影平面： \mathbb{F}_q^3 における直線

- ▶ \mathbb{F}_q^3 において，原点 $(0, 0, 0)$ を通る直線は，
 $(a, b, c) \in \mathbb{F}_q^3 - \{0\}$ を使って

$$\{(x, y, z) \mid \text{ある } k \in \mathbb{F}_q \text{ が存在して, } x = ka, y = kb, z = kc\}$$

と書ける (これを $L(a, b, c)$ とする)

考えるべきこと

異なる (a, b, c) に対して，異なる直線が得られるか？

\mathbb{F}_q 上の射影平面： \mathbb{F}_q^3 における直線 (2)

例： $q = 3$ のとき, \mathbb{F}_3 において

$$\begin{aligned} L(2, 1, 1) &= \{(x, y, z) \mid \exists k \in \mathbb{F}_3 : x = 2k, y = k, z = k\} \\ &= \{(0, 0, 0), (2, 1, 1), (1, 2, 2)\} \\ &= \{(x, y, z) \mid \exists k \in \mathbb{F}_3 : x = k, y = 2k, z = 2k\} \end{aligned}$$

例： $q = 5$ のとき, \mathbb{F}_5 において

$$\begin{aligned} L(4, 1, 3) &= \{(x, y, z) \mid \exists k \in \mathbb{F}_5 : x = 4k, y = k, z = 3k\} \\ &= \{(0, 0, 0), (4, 1, 3), (3, 2, 1), (2, 3, 4), (1, 4, 2)\} \\ &= \{(x, y, z) \mid \exists k \in \mathbb{F}_5 : x = k, y = 4k, z = 2k\} \\ &= \{(x, y, z) \mid \exists k \in \mathbb{F}_5 : x = 2k, y = 3k, z = 4k\} \\ &= \{(x, y, z) \mid \exists k \in \mathbb{F}_5 : x = 3k, y = 2k, z = k\} \end{aligned}$$

つまり, 同じ直線がちょうど $q - 1$ 個だけ現れる?

\mathbb{F}_q 上の射影平面： \mathbb{F}_q^3 における直線の数性質： \mathbb{F}_q^3 における原点を通る直線の数はいくつ？

$$\frac{q^3 - 1}{q - 1} \quad (\text{すなわち, } q^2 + q + 1)$$

例

- ▶ $q = 2 : q^2 + q + 1 = 7$
- ▶ $q = 3 : q^2 + q + 1 = 13$
- ▶ $q = 4 : q^2 + q + 1 = 21$
- ▶ $q = 5 : q^2 + q + 1 = 31$

\mathbb{F}_q 上の射影平面： \mathbb{F}_q^3 における直線の数 (補題)

まず、次の補題を証明する

補題 L

任意の $(a, b, c), (a', b', c') \in \mathbb{F}_q^3 - \{\mathbf{0}\}$ に対して

$$L(a, b, c) = L(a', b', c') \Leftrightarrow \begin{array}{l} \text{ある } \lambda \in \mathbb{F}_q - \{0\} \text{ が存在して,} \\ a = \lambda a', b = \lambda b', c = \lambda c' \end{array}$$

⇐ の証明：そのような λ が存在すると仮定。このとき、

$$\begin{aligned} L(a, b, c) &= \{(x, y, z) \mid \exists k \in \mathbb{F}_q : x = ka, y = kb, z = kc\} \\ &= \{(x, y, z) \mid \exists k \in \mathbb{F}_q : x = k\lambda a', y = k\lambda b', z = k\lambda c'\} \\ &= \{(x, y, z) \mid \exists k' \in \mathbb{F}_q : x = k'a', y = k'b', z = k'c'\} \\ &= L(a', b', c') \end{aligned}$$

□

注： $k \mapsto k\lambda$ は \mathbb{F}_q 上の全単射 ($\because k \mapsto k\lambda^{-1}$ が逆写像)

\mathbb{F}_q 上の射影平面： \mathbb{F}_q^3 における直線の数 (補題) 続

まず、次の補題を証明する

補題 L

任意の $(a, b, c), (a', b', c') \in \mathbb{F}_q^3 - \{0\}$ に対して

$$L(a, b, c) = L(a', b', c') \Leftrightarrow \begin{array}{l} \text{ある } \lambda \in \mathbb{F}_q - \{0\} \text{ が存在して,} \\ a = \lambda a', b = \lambda b', c = \lambda c' \end{array}$$

\Rightarrow の証明： $L(a, b, c) = L(a', b', c')$ であると仮定

- ▶ 特に, $(a', b', c') \in L(a', b', c') = L(a, b, c)$
- ▶ ある $k \in \mathbb{F}_q - \{0\}$ が存在して, $a' = ka, b' = kb, c' = kc$ □

\mathbb{F}_q 上の射影平面： \mathbb{F}_q^3 における直線 (証明) \mathbb{F}_q^3 における原点を通る直線の数は？

$$\frac{q^3 - 1}{q - 1} \quad (\text{すなわち, } q^2 + q + 1)$$

証明：

- ▶ $|\mathbb{F}_q^3 - \{\mathbf{0}\}| = q^3 - 1$
- ▶ 補題 L より, その中の $q - 1$ 個の要素は同じ直線を与える
- ▶ したがって, 異なる直線の本数は $\frac{q^3 - 1}{q - 1}$ □

\mathbb{F}_q 上の射影平面： \mathbb{F}_q^3 における平面

- ▶ \mathbb{F}_q^3 において，原点 $(0, 0, 0)$ を通る平面は，
 $(a, b, c) \in \mathbb{F}_q^3 - \{0\}$ を使って

$$\{(x, y, z) \mid ax + by + cz = 0\}$$

と書ける (これを $P(a, b, c)$ をする)

考えるべきこと

異なる (a, b, c) に対して，異なる平面が得られるか？

\mathbb{F}_q 上の射影平面： \mathbb{F}_q^3 における平面 (2)

例： $q = 3$ のとき, \mathbb{F}_3 において

$$\begin{aligned} 2x + y + z = 0 &\Leftrightarrow 2 \cdot (2x + y + z) = 2 \cdot 0 \\ &\Leftrightarrow x + 2y + 2z = 0 \end{aligned}$$

例： $q = 5$ のとき, \mathbb{F}_5 において

$$\begin{aligned} 4x + y + 3z = 0 &\Leftrightarrow 2 \cdot (4x + y + 3z) = 2 \cdot 0 &\Leftrightarrow 3x + 2y + z = 0 \\ &\Leftrightarrow 3 \cdot (4x + y + 3z) = 3 \cdot 0 &\Leftrightarrow 2x + 3y + 4z = 0 \\ &\Leftrightarrow 4 \cdot (4x + y + 3z) = 4 \cdot 0 &\Leftrightarrow x + 4y + 2z = 0 \end{aligned}$$

同じ平面がちょうど $q - 1$ 個だけ現れる？

\mathbb{F}_q 上の射影平面： \mathbb{F}_q^3 における平面の数

\mathbb{F}_q^3 における原点を通る平面の数は？

$$\frac{q^3 - 1}{q - 1} \quad (\text{すなわち, } q^2 + q + 1)$$

例

- ▶ $q = 2 : q^2 + q + 1 = 7$
- ▶ $q = 3 : q^2 + q + 1 = 13$
- ▶ $q = 4 : q^2 + q + 1 = 21$
- ▶ $q = 5 : q^2 + q + 1 = 31$

\mathbb{F}_q 上の射影平面： \mathbb{F}_q^3 における平面の数 (補題)

まず、次の補題を証明する

補題 P

任意の $(a, b, c), (a', b', c') \in \mathbb{F}_q^3 - \{0\}$ に対して

$$P(a, b, c) = P(a', b', c') \Leftrightarrow \begin{array}{l} \text{ある } \lambda \in \mathbb{F}_q - \{0\} \text{ が存在して,} \\ a = \lambda a', b = \lambda b', c = \lambda c' \end{array}$$

\Leftarrow の証明：そのような λ が存在すると仮定。このとき、

$$\begin{aligned} P(a, b, c) &= \{(x, y, z) \mid ax + by + cz = 0\} \\ &= \{(x, y, z) \mid \lambda a'x + \lambda b'y + \lambda c'z = 0\} \\ &= \{(x, y, z) \mid a'x + b'y + c'z = 0\} \\ &= P(a', b', c') \end{aligned}$$

□

\mathbb{F}_q 上の射影平面： \mathbb{F}_q^3 における平面の数 (補題) 続

まず、次の補題を証明する

補題 P

任意の $(a, b, c), (a', b', c') \in \mathbb{F}_q^3 - \{0\}$ に対して

$$P(a, b, c) = P(a', b', c') \Leftrightarrow \begin{array}{l} \text{ある } \lambda \in \mathbb{F}_q - \{0\} \text{ が存在して,} \\ a = \lambda a', b = \lambda b', c = \lambda c' \end{array}$$

\Rightarrow の証明： $P(a, b, c) = P(a', b', c')$ を仮定

- ▶ $a \neq 0$ と仮定 ($b \neq 0$ や $c \neq 0$ の場合も同様に証明できる)
- ▶ $\lambda = a'a^{-1}$ とする (つまり, $a' = \lambda a$)
- ▶ $(a^{-1}b, -1, 0), (a^{-1}c, 0, -1) \in P(a, b, c) = P(a', b', c')$ である (なぜ?)

\mathbb{F}_q 上の射影平面： \mathbb{F}_q^3 における平面の数 (補題) 続

まず、次の補題を証明する

補題 P

任意の $(a, b, c), (a', b', c') \in \mathbb{F}_q^3 - \{0\}$ に対して

$$P(a, b, c) = P(a', b', c') \Leftrightarrow \begin{array}{l} \text{ある } \lambda \in \mathbb{F}_q - \{0\} \text{ が存在して,} \\ a = \lambda a', b = \lambda b', c = \lambda c' \end{array}$$

\Rightarrow の証明： $P(a, b, c) = P(a', b', c')$ を仮定

- ▶ $a \neq 0$ と仮定 ($b \neq 0$ や $c \neq 0$ の場合も同様に証明できる)
- ▶ $\lambda = a'a^{-1}$ とする (つまり, $a' = \lambda a$)
- ▶ $(a^{-1}b, -1, 0), (a^{-1}c, 0, -1) \in P(a, b, c) = P(a', b', c')$ である (なぜ?)
- ▶ 仮定より, $a' \cdot (a^{-1}b) + b' \cdot (-1) = 0$, $a' \cdot (a^{-1}c) + c' \cdot (-1) = 0$
- ▶ このとき, $b' = a'a^{-1}b = \lambda b$ であり, $c' = a'a^{-1}c = \lambda c$ □

\mathbb{F}_q 上の射影平面： \mathbb{F}_q^3 における平面（証明）

\mathbb{F}_q^3 における原点を通る平面の数は？

$$\frac{q^3 - 1}{q - 1} \quad (\text{すなわち, } q^2 + q + 1)$$

証明：

- ▶ $|\mathbb{F}_q^3 - \{\mathbf{0}\}| = q^3 - 1$
- ▶ 補題 P より、その中の $q - 1$ 個の要素は同じ平面を与える
- ▶ したがって、異なる平面の数は $\frac{q^3 - 1}{q - 1}$ □

2つの直線を含む平面は一意に存在

次のことを証明する

性質：2つの直線を含む平面は一意に存在

任意の異なる $(a, b, c), (a', b', c') \in \mathbb{F}_q^3 - \{\mathbf{0}\}$ に対して,
 $L(a, b, c)$ と $L(a', b', c')$ が異なるとき,
ある $(a'', b'', c'') \in \mathbb{F}_q^3 - \{\mathbf{0}\}$ が存在して,

$$L(a, b, c) \subseteq P(a'', b'', c''), \quad L(a', b', c') \subseteq P(a'', b'', c'')$$

そのような (a'', b'', c'') はスカラー倍を除いて一意

2つの直線を含む平面は一意に存在：存在性

性質：2つの直線を含む平面は一意に存在

任意の異なる $(a, b, c), (a', b', c') \in \mathbb{F}_q^3 - \{0\}$ に対して,
 $L(a, b, c)$ と $L(a', b', c')$ が異なるとき,
 ある $(a'', b'', c'') \in \mathbb{F}_q^3 - \{0\}$ が存在して,

$$L(a, b, c) \subseteq P(a'', b'', c''), \quad L(a', b', c') \subseteq P(a'', b'', c'')$$

そのような (a'', b'', c'') はスカラー倍を除いて一意

証明 (存在性)：仮定を満たす $(a, b, c), (a', b', c') \in \mathbb{F}_q^3 - \{0\}$ を考える

- ▶ $a'' = bc' - b'c, b'' = ca' - c'a, c'' = ab' - a'b$ とおく
- ▶ このとき, $(a'', b'', c'') \neq 0$ (なぜ?)

2つの直線を含む平面は一意に存在：存在性

性質：2つの直線を含む平面は一意に存在

任意の異なる $(a, b, c), (a', b', c') \in \mathbb{F}_q^3 - \{0\}$ に対して,
 $L(a, b, c)$ と $L(a', b', c')$ が異なるとき,
 ある $(a'', b'', c'') \in \mathbb{F}_q^3 - \{0\}$ が存在して,

$$L(a, b, c) \subseteq P(a'', b'', c''), \quad L(a', b', c') \subseteq P(a'', b'', c'')$$

そのような (a'', b'', c'') はスカラー倍を除いて一意

証明 (存在性)：仮定を満たす $(a, b, c), (a', b', c') \in \mathbb{F}_q^3 - \{0\}$ を考える

- ▶ $a'' = bc' - b'c, b'' = ca' - c'a, c'' = ab' - a'b$ とおく
- ▶ このとき, $(a'', b'', c'') \neq 0$ (なぜ?)
- ▶ さらに, $a''a + b''b + c''c = 0$ かつ $a''a' + b''b' + c''c' = 0$

2つの直線を含む平面は一意に存在：存在性

性質：2つの直線を含む平面は一意に存在

任意の異なる $(a, b, c), (a', b', c') \in \mathbb{F}_q^3 - \{\mathbf{0}\}$ に対して,
 $L(a, b, c)$ と $L(a', b', c')$ が異なるとき,
 ある $(a'', b'', c'') \in \mathbb{F}_q^3 - \{\mathbf{0}\}$ が存在して,

$$L(a, b, c) \subseteq P(a'', b'', c''), \quad L(a', b', c') \subseteq P(a'', b'', c'')$$

そのような (a'', b'', c'') はスカラー倍を除いて一意

証明 (存在性)：仮定を満たす $(a, b, c), (a', b', c') \in \mathbb{F}_q^3 - \{\mathbf{0}\}$ を考える

- ▶ $a'' = bc' - b'c, b'' = ca' - c'a, c'' = ab' - a'b$ とおく
- ▶ このとき, $(a'', b'', c'') \neq \mathbf{0}$ (なぜ?)
- ▶ さらに, $a''a + b''b + c''c = 0$ かつ $a''a' + b''b' + c''c' = 0$
- ▶ したがって, $L(a, b, c) \subseteq P(a'', b'', c'')$ かつ
 $L(a', b', c') \subseteq P(a'', b'', c'')$

□

2つの直線を含む平面は一意に存在：一意性 (1)

性質：2つの直線を含む平面は一意に存在

任意の異なる $(a, b, c), (a', b', c') \in \mathbb{F}_q^3 - \{0\}$ に対して,
 $L(a, b, c)$ と $L(a', b', c')$ が異なるとき,
 ある $(a'', b'', c'') \in \mathbb{F}_q^3 - \{0\}$ が存在して,

$$L(a, b, c) \subseteq P(a'', b'', c''), \quad L(a', b', c') \subseteq P(a'', b'', c'')$$

そのような (a'', b'', c'') はスカラー倍を除いて一意

証明 (一意性)：異なる $(a, b, c), (a', b', c') \in \mathbb{F}_q^3 - \{0\}$ を考える

- ▶ (a'', b'', c'') が条件を満たすとする
- ▶ このとき,

$$a'' \cdot a + b'' \cdot b + c'' \cdot c = 0, \quad (1)$$

$$a'' \cdot a' + b'' \cdot b' + c'' \cdot c' = 0 \quad (2)$$

2つの直線を含む平面は一意に存在：一意性 (2)

証明 (一意性)：異なる $(a, b, c), (a', b', c') \in \mathbb{F}_q^3 - \{\mathbf{0}\}$ を考える

- ▶ (a'', b'', c'') が条件を満たすとする
- ▶ このとき,

$$a'' \cdot a + b'' \cdot b + c'' \cdot c = 0, \quad (1)$$

$$a'' \cdot a' + b'' \cdot b' + c'' \cdot c' = 0 \quad (2)$$

2つの直線を含む平面は一意に存在：一意性 (2)

証明 (一意性)：異なる $(a, b, c), (a', b', c') \in \mathbb{F}_q^3 - \{0\}$ を考える

- ▶ (a'', b'', c'') が条件を満たすとする
- ▶ このとき,

$$a'' \cdot a + b'' \cdot b + c'' \cdot c = 0, \quad (1)$$

$$a'' \cdot a' + b'' \cdot b' + c'' \cdot c' = 0 \quad (2)$$

- ▶ $a \neq 0$ のときを考える ($b \neq 0, c \neq 0$ のときも同様)
- ▶ このとき, 式 (1) より, $a'' = -a^{-1}(b''b + c''c)$
- ▶ これと式 (2) より, $-a^{-1}(b''b + c''c)a' + b''b' + c''c' = 0$

2つの直線を含む平面は一意的に存在：一意性 (2)

証明 (一意性)：異なる $(a, b, c), (a', b', c') \in \mathbb{F}_q^3 - \{0\}$ を考える

- ▶ (a'', b'', c'') が条件を満たすとする
- ▶ このとき,

$$a'' \cdot a + b'' \cdot b + c'' \cdot c = 0, \quad (1)$$

$$a'' \cdot a' + b'' \cdot b' + c'' \cdot c' = 0 \quad (2)$$

- ▶ $a \neq 0$ のときを考える ($b \neq 0, c \neq 0$ のときも同様)
- ▶ このとき, 式 (1) より, $a'' = -a^{-1}(b''b + c''c)$
- ▶ これと式 (2) より, $-a^{-1}(b''b + c''c)a' + b''b' + c''c' = 0$
- ▶ $\therefore (a'b - ab')b'' = (c'a - ca')c''$
- ▶ つまり, ある $k \in \mathbb{F}_q$ が存在して, $b'' = k(c'a - ca'), c'' = k(a'b - ab')$
- ▶ このとき,

$$a'' = -a^{-1}(k(c'a - ca')b + k(a'b - ab')c) = k(b'c - bc')$$

□

2つの平面に含まれる直線は一意に存在

次の性質の証明は演習問題

性質：2つの平面に含まれる直線は一意に存在

任意の異なる $(a, b, c), (a', b', c') \in \mathbb{F}_q^3 - \{\mathbf{0}\}$ に対して,
 $P(a, b, c)$ と $P(a', b', c')$ が異なるとき,
ある $(a'', b'', c'') \in \mathbb{F}_q^3 - \{\mathbf{0}\}$ が存在して,

$$L(a'', b'', c'') \subseteq P(a, b, c), \quad L(a'', b'', c'') \subseteq P(a', b', c')$$

そのような (a'', b'', c'') はスカラー倍を除いて一意

\mathbb{F}_q 上の射影平面：まとめ \mathbb{F}_q^3 において

- ▶ 原点を通る直線の数 = $q^2 + q + 1$
- ▶ 原点を通る平面の数 = $q^2 + q + 1$
- ▶ 原点を通る 2 平面が含む, 原点を通る直線の数 = 1
- ▶ 原点を通る 2 直線を含む, 原点を通る平面の数 = 1

ここで作った直線と平面の集合を \mathbb{F}_q 上の射影平面 と呼ぶ

問題：次の性質を満たす集合の集合は存在するか？

正整数 m, q , 有限集合 X , $|X| = v$

問題

m 個の集合 $A_1, A_2, \dots, A_m \subseteq X$ で次を満たすものは存在するか？

- ▶ $|A_1| = |A_2| = \dots = |A_m| = q + 1$
- ▶ 任意の異なる $i, j \in \{1, 2, \dots, m\}$ に対して
 $x \in A_i \cap A_j$ となる $x \in X$ が一意に存在する
- ▶ 任意の異なる $x, y \in X$ に対して
 $x, y \in A_i$ となる $i \in \{1, 2, \dots, m\}$ が一意に存在する

\mathbb{F}_q 上の射影平面を考えることで、次の場合の存在が分かる

- ▶ q は素数のべき, $m = q^2 + q + 1$, $v = q^2 + q + 1$

目次

- ① 有限射影平面：例
- ② 有限射影平面：構成
- ③ 有限射影平面：一般
- ④ 今日のまとめ

問題：次の性質を満たす集合の集合は存在するか？

正整数 m, q , 有限集合 X , $|X| = v$

問題

m 個の集合 $A_1, A_2, \dots, A_m \subseteq X$ で次を満たすものは存在するか？

- ▶ $|A_1| = |A_2| = \dots = |A_m| = q + 1$
- ▶ 任意の異なる $i, j \in \{1, 2, \dots, m\}$ に対して
 $x \in A_i \cap A_j$ となる $x \in X$ が一意に存在する
- ▶ 任意の異なる $x, y \in X$ に対して
 $x, y \in A_i$ となる $i \in \{1, 2, \dots, m\}$ が一意に存在する

定義：有限射影平面

$v = m = q^2 + q + 1$ のとき,
これを満たすものを **位数 q の有限射影平面** と呼ぶ

ここまでのまとめ： q が素数のべき \Rightarrow 位数 q の有限射影平面は存在

有限射影平面：未解決問題

定義：有限射影平面

$v = m = q^2 + q + 1$ のとき,
これを満たすものを **位数 q の有限射影平面** と呼ぶ

ここまでのまとめ： q が素数のべき \Rightarrow 位数 q の有限射影平面は存在

未解決問題：次は正しいか？

位数 q の有限射影平面が存在 $\Rightarrow q$ は素数のべき

知られていること

- ▶ $q = 6$ のときは存在しない
- ▶ $q = 10$ のときは存在しない (Lam '91)
- ▶ $q = 12$ のときに存在しないか、未解決
- ▶ $q = 14$ のときは存在しない

非存在について, Bruck-Ryser の定理 ('49) が知られている (内容は省略)

目次

- ① 有限射影平面：例
- ② 有限射影平面：構成
- ③ 有限射影平面：一般
- ④ 今日のまとめ

今日のまとめ

今日の目標

有限射影平面について次ができるようになる

- ▶ 有限体を用いて構成できるようになる
- ▶ 基本的な性質を証明できるようになる

有限射影平面の一般化として、より次元の高い有限射影空間を考えることもできる
(ただ、平面の場合よりもかなりややこしい)

目次

- ① 有限射影平面：例
- ② 有限射影平面：構成
- ③ 有限射影平面：一般
- ④ 今日のまとめ